TUNKEUTUMISEN HAVAITSEMIS-JÄRJESTELMÄN KÄYTTÖÖNOTTO

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2006
Mika Luukkanen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

LUUKKANEN, MIKA: Tunkeutumisen havaitsemisjärjestelmän käyttöönotto

Tietoliikennetekniikan opinnäytetyö, 56 sivua, 23 liitesivua

Kevät 2006

TIIVISTELMÄ

Tämä opinnäytetyö käsittelee tunkeutumisen havaitsemisjärjestelmiä, niiden taustoja ja itse ohjelman käyttöönottoa Päijät-Hämeen koulutuskonsernin tietohallintopalveluille.

Teoriaosuudessa käydään, läpi minkälaisia tietoturvauhkia on nykyään olemassa. Lisäksi katsotaan, mistä ja miten tunkeutumisen havaitsemisjärjestelmät ovat kehittyneet niiden alkuajoista lähtien. Tunkeutumisen havaitsemisjärjestelmät voidaan jakaa kahteen päätyyppiin: Tässä työssä keskitytään verkkoon asennettavaan erilliseen laitteeseen. Olemassa on myös työasema/palvelinkoneeseen asennettavia tunkeutumisen havaitsemisohjelmistoja, jotka suojelevat vain kyseistä laitetta. Tämän työn lähtökohtana oli saada toteutettua laite, joka tutkii verkon liikennettä.

Snort-ohjelmaan päätyminen oli lopulta melko helppo ratkaisu. Ohjelma perustuu vapaaseen lähdekoodiin ja toimii lisäksi linux-käyttöjärjestelmissä. Ohjelman kehitys on myös jatkuvaa, ja päivityksiä ilmestyy tasaiseen tahtiin. Säännöt päivitetään nopeasti heti uuden uhan ilmestyessä. Snort-ohjelmalla on myös todella laaja käyttäjäkunta maailmalla, joten ongelmatilanteissa ratkaisu löytyy helposti. Snort-kirjoja on olemassa toistakymmentä erilaista, jos haluaa syventyä aiheeseen tarkemmin kuin pelkästään ohjelman manuaalien avulla.

Käytännön kokeissa havaittiin että Snort tarjoaa erittäin paljon lisätietoa verkossa liikkuvista paketeista ja varsinkin siellä olevasta epämääräisestä liikenteestä. Näillä tiedoilla voidaan tutkia mihin hyökkäykset verkossa kohdistuvat ja yrittää parantaa verkon tietoturvaa.

Asiasanat: Tietoturva, IDS, Snort, tunkeutumisen havaitseminen

Lahti University of Applied Sciences
Faculty of Technology

LUUKKANEN, MIKA: The implementation of an Intrusion Detection System

Bachelor's Thesis in Telecommunications Technology, 56 pages, 23 appendices

Spring 2006

ABSTRACT

This thesis deals with intrusion detection systems, their backgrounds, and the implementation of the system for the IT services of Lahti Region Educational Consortium.

The theory part examines what kinds of data security threats there are. There is also a survey of how intrusion detection systems have developed from their early ages. You can group intrusion detection systems to two main types. This thesis concentrates on devices that are installed in networks. There also exist intrusion detection systems that are installed in servers/workstations, and the system only protects that device. The starting point for this thesis was to implement a device that detects networks traffic.

It was eventually an easy decision to end up with the Snort system. The program is based on open source and works in the Linux systems. Program development is continuous and updates appear constantly. Rule files are updated quickly after a new threat emerges up. The Snort program has a very broad range of users in the world, so it is easy to find a solution in problem situations. There are also dozens of books about Snort, if you want to know more than the manuals tell.

In practical tests it was discovered that Snort gives lots of information about packets in the network and especially obscure traffic that moves in the network. With these facts you can inspect where attacks are aimed at in the network and try to improve the security of the network.

Keywords: security, IDS, Snort, intrusion detection

SISÄLLYS

LYHENNELUETTELO

DMZ	Demilitarized zone. Verkon puskurialue Internetin ja lähiverkon välissä. Alueen tarkoitus on estää kaikki suorat yhteysyritykset lähiverkkoon ja suojata lähiverkkoa Internetistä tehdyiltä hyökkäyksiltä.
DNS	Domain name service. Internetin nimipalvelujärjestelmä, joka muuntaa Internetin verkkotunnukset kommunikaation mahdollistaviksi IP-osoitteiksi.
FTP	File transfer protocol. TCP-protokollaa käyttävä tiedostonsiirtomenetelmä kahden tietokoneen välille.
HIDS	Host intrusion detection system. Laitekohtainen tunkeutumisen havaitsemisjärjestelmä, joka valvoo vain itse laitetta.
HTTP	Hypertext transfer protocol. Web-sivujen siirtokäytäntö TCP/IP-verkossa.
HTTPS	Hypertext transfer protocol secure. HTTP-protokollan salattu versio.
ICMP	Internet control message protocol. TCP/IP-pinon kontrolliprotokolla, jolla lähetetään virheilmoituksia ja tiedotusviestejä koneesta toiseen.
IDS	Intrusion detection system. Tietoverkkoon asennettava järjestelmä, joka on ohjelmoitu tunnistamaan verkkoon suuntautuvat hyökkäysyritykset.

IP-osoite	Internet protocol. Verkkokerroksen tietoliikenneosoite, esimerkiksi Internetissä IPv4-standardin mukaisesti liikennöivälle laitteelle annettu 32-bittinen hierarkkinen, neliosainen osoite.
MAC-osoite	Media access control. Verkkosovittimen ethernet-verkossa yksilöivä osoite.
NIDS	Network intrusion detection system. Tunkeutumisen havaitsemisjärjestelmä joka valvoo verkkoa tai aliverkkoa.
P2P	Peer to peer, Tietokoneverkko, jossa ei ole kiinteitä palvelimia ja asiakkaita, vaan jokainen verkkoon kytketty kone toimii sekä palvelimena että asiakkaana verkon muille koneille.
RFC	Request for comments. Internet-verkossa sen liikennekäytäntöjä sekä niihin liittyviä kokeiluja kootusti esittelevä asiakirjasarja, joka sisältää mm. IETF- eli Internet-standardit.
RPC	Remote procedure call. Käytetään tietokoneiden ja niissä suoritettavien ohjelmien väliseen tiedonvälitykseen.
SMTP	Simple mail transfer protocol. TCP-pohjainen protokolla, jota käytetään sähköpostiviestien lähettämiseen ja vastaanottamiseen.
SSH	Secure shell. Suomessa kehitetty suojattu yhteyskäytäntö, joka perustuu hybridisalaukseen. Viesti salakirjoitetaan satunnaisella symmetrisellä kerta-

	avaimella, joka lähetetään vastaanottajalle tämän julkisella avaimella salattuna.
TCP	Transmission control protocol. Yhteydellinen tietoliikenneprotokolla, jolla luodaan Internet-tietokoneiden välille yhteyksiä.
TFTP	Trivial file transfer protocol. Tiedonsiirtoprotokolla, jota käytetään yleisesti laitteiden ohjelmistopäivityksissä.
UDP	User datagram protocol. Yhteydetön tietoliikenneprotokolla, jolla sovellus voi lähettää viestejä toiselle tietokoneelle.
VLAN	Virtual local area network. Tekniikka, jolla fyysinen tietoliikenneverkko voidaan jakaa loogisiin osiin.
XML	Extensible markup language. Metakieli, eli kieli jolla voidaan kuvata toisia kieliä. XML muistuttaa HTML-kieltä, jolla WWW-sivut kirjoitetaan.

1. JOHDANTO

Tämän opinnäytetyön tavoitteena on kartoittaa Päijät-Hämeen koulutuskonsernin tietohallinnon tarpeisiin sopiva tunkeutumisen havaitsemisjärjestelmä ja huolehtia sen asennuksesta ja käyttöönotosta. Laitteen valinnassa keskitytään laitteen ominaisuuksiin, käytettävyyteen ja kustannuksiin. Toiveena oli myös, että tuote olisi avoimen lähdekoodin ohjelmisto ja toimintaympäristönä olisi linux.

Kuten monet esimerkit ovat osoittaneet, on verkoissa paljon epämääräistä liikennettä, jonka havaitseminen ja estäminen on tärkeää normaalin liikenteen turvaamiseksi. Tarkoituksena on muun muassa tutkia, mitä uhkia DMZ-alueen palvelimet joutuvat kohtaamaan. Nämä palvelimet tarjoavat palveluita ulkomaailmaan ja ovat selkeä kohde Internetistä tuleville hyökkäyksille.

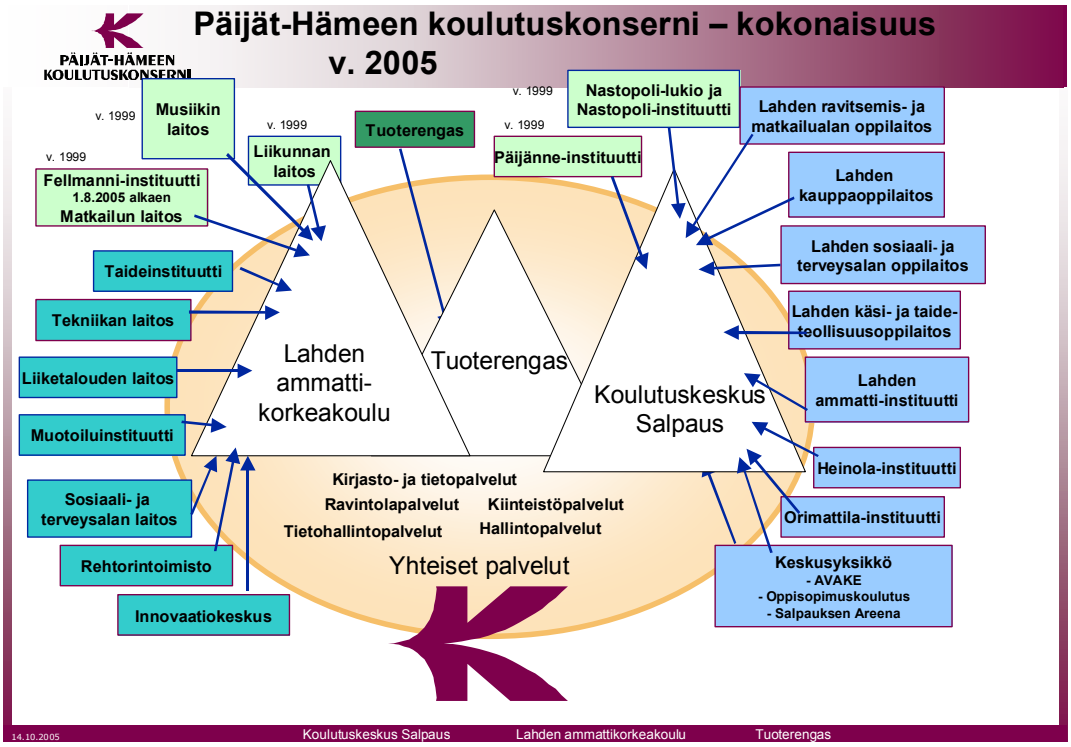
Tunkeutumisen havaitsemisjärjestelmän keräämien tietojen avulla on tarkoitus pystyä raportoimaan entistä tarkemmin palomuurien tarpeellisuudesta ja tehosta. Havainnointia voidaan suorittaa verkon eri paikoista, jotta saadaan vertailutuloksia. Järjestelmällä on myös tavoitteena saada yksityiskohtaisia tietoja siitä, minkä tyyppisiä hyökkäyksiä verkossa liikkuu, jotta tiedetään, mitä vastaan verkossa olevat laitteet tulee suojata.

Samalla halutaan että hyökkäyksistä olisi tiedot helposti saatavilla myös pidemmältä aikajaksolta, jolloin voidaan huomata esimerkiksi eri hyökkäysten mahdolliset riippuvuudet ja jotta voidaan havaita, jos hyökkäyksissä toistuu jokin säännöllinen kuvio.

2. PÄIJÄT-HÄMEEN KOULUTUSKONSERNI

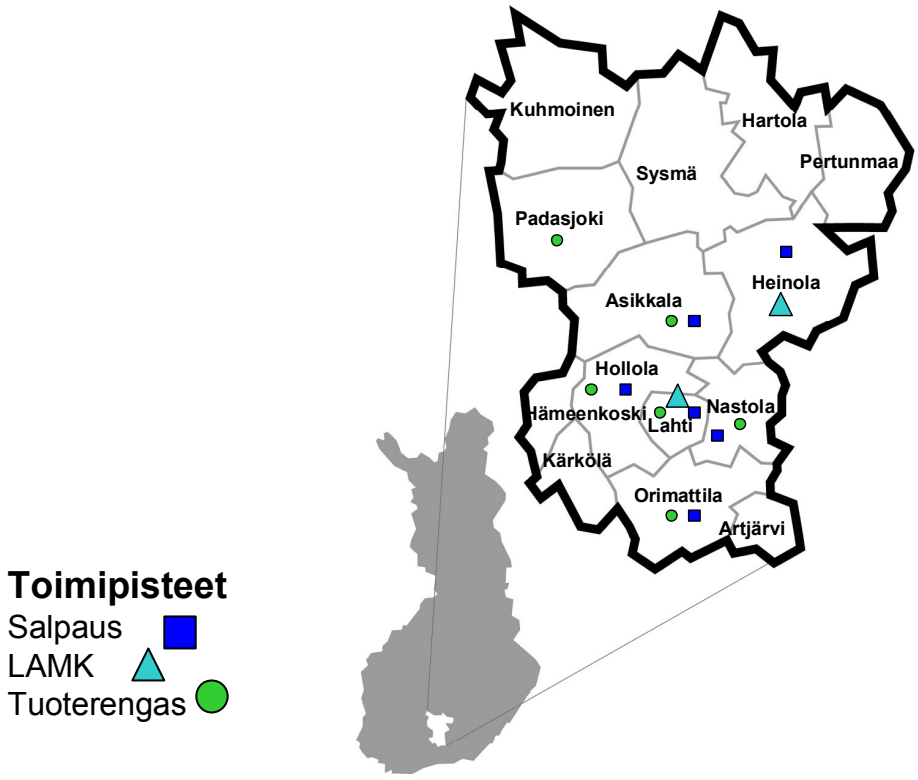
2.1 Yleistä PHKK:sta

Päijät-Hämeen koulutuskonserni on maakunnallinen koulutuksen järjestäjä, kehittäjä ja ylläpitäjä. Koulutuskonserni johtaa ja koordinoi jäsenkuntiensa puolesta ammattikorkeakoulutusta, ammatillista koulutusta, oppisopimuskoulutusta sekä kuntoutusta ja työhönvalmennusta. (Päijät-Hämeen koulutuskonserni, toimintamalli 2005.)



Kuvio 1. Päijät-Hämeen koulutuskonserni – kokonaisuus (PHKK – esittelykalvosarja 2005)

Päijät-Hämeen koulutuskonserni-kuntayhtymään kuuluu 14 jäsenkuntaa, jotka ovat Artjärvi, Asikkala, Hartola, Heinola, Hollola, Hämeenkoski, Kuhmoinen, Kärkölä, Lahti, Nastola, Orimattila, Padasjoki, Pertunmaa ja Sysmä. (PHKK esittelykalvosarja 2005, 4.)



Kuvio 2. Päijät-Hämeen koulutuskonsernin jäsenkunnat ja toimialue (PHKK – esittelykalvosarja 2005)

Koulutuskeskus Salpaus, Lahden ammattikorkeakoulu ja Tuoterengas ovat Päijät-Hämeen koulutuskonsernin liikelaitoksia. Lisäksi koulutuskonsernilla toimii sisäisinä palveluyksikköinä Yhteiset palvelut, joita ovat Hallintopalvelut, Kirjasto- ja tietopalvelut, Kiinteistöpalvelut, Ravintolapalvelut ja Tietohallintopalvelut. (Päijät-Hämeen koulutuskonserni, toimintamalli 2005.)

Päätoimisia opiskelijoita konsernissa vuonna 2004 oli 11.669 henkilöä, joista 7718 Koulutuskeskus Salpauksessa ja 3951 Lahden Ammattikorkeakoulussa. Koulutuskonsernin koko henkilöstön määrä vuonna 2004 oli yhteensä 1606 henkilöä. Konsernin budjetti samana vuonna oli 99 miljoonaa euroa. (Tunnuslukuja Päijät-Hämeen koulutuskonsernista 2004.)

2.2 PHKK:n tietohallintopalvelut

Liikelaitosten toimipisteet on liitetty Päijät-Hämeen koulutuskonsernin runkoverkkoon 1Gbit/s nopeudella. Ja vuodesta 2005 lähtien myös etäpaikat ovat saaneet 1Gbit/s yhteysnopeuden uuden tietoliikennesopimuksen myötä. Liitteessä 1 näkyy PHKK:n verkon looginen rakenne.

FUNETin (Finnish University and Research Network) verkkoon yhteys PHKK:n runkoverkosta on 1Gbit/s. Suojaus on toteutettu kahdennetuilla palomuureilla. Koulutuskeskus Salpaus ja PHKK:n yhteiset palvelut käyttävät toista Internet-yhteyttä, jonka toimittaa PHNet. Liikennöitäessä kotimaassa on yhteyden nopeus 40Mbit/s ja ulkomaille 10Mbit/s. Suurin osa eri toimipisteiden lähiverkoista toimii 100Mbit/s nopeudella. Tärkeimpiä lähiverkkojen yhteysvälejä on päivitetty 1Gbit/s nopeuteen, ja olemassa on myös alle 100 Mbit/s yhteyksiä, jotka on tarkoitus päivittää nopeammiksi. (Päijät-Hämeen koulutuskonsernin tietoverkko 2005.)

Päijät-Hämeen puhelimelta (PHP) on vuodesta 2005 lähtien ostettu palveluna runkoverkon eri toimipisteet yhdistävät laitteet ylläpitoineen. Lähiverkkojen kytkimet ovat pääasiassa hallittavia, ja ei-hallittavia kytkimiä kaikista kytkimistä on noin kolmannes. PHKK:n tietohallintopalvelut vastaa verkon valvonnasta. Lähiverkkojen osalta kaapelointi on toteutettu Cat5-standardin mukaan. Uusissa kaapeloinneissa käytetään Cat6-standardin mukaisia kaapeleita. Valokuituyhteyksiä käytetään pitkissä yhteysväleissä mukaan lukien koko runkoverkko, sekä 1 Gbit/s segmenteissä. (Päijät-Hämeen koulutuskonsernin tietoverkko 2005.)

Tietohallintopalvelut hallinnoi keskitetysti tietoverkkoa. Tietohallintopalveluiden tehtävinä on tietohallinnon kehittäminen, tietohallintoon liittyvien sopimusten ja hankintojen koordinointi, tietojärjestelmien kehittäminen ja tekninen ylläpito, tietoliikennepalvelut (data- ja puhelinliikenne), IT-tukipalvelujen ylläpito ja kehittäminen, tietoteknisen tietoturvan ylläpito ja kehittäminen, puhelinpalveluiden koordinointi ja puhelunvälitys.

Hakemistopalveluna on käytetty vuodesta 2001 lähtien Microsoft Active Directorya, josta löytyvät Lahden ammattikorkeakoulun käyttäjät, työasemat, palvelimet ja muut objektit. (Päijät-Hämeen koulutuskonsernin tietoverkko 2005.)

Työasemia konsernilla oli vuonna 2005 yhteensä 4622 kpl, joista opiskelijoiden käytössä on 3030 ja henkilökunnan käytössä 1592. Vuodelta 2006 ei ole tarkkoja lukuja, mutta työasemien määrä on noussut yli 5000 kappaleen. (PHKK esittelykalvosarja 2005, 11.)

3.VERKKOUHAT

Tietoverkkohyökkäykset ovat yleistyneet niin paljon, että jokaisen verkossa liikkujan tulisi ottaa huomioon tietoturvakysymykset. Nykyään kun lähes jokaisella on mahdollisuus hankkia kotiin laajakaistaliittymä ja tietokoneesta on tullut joka kotiin hankittava yleiskone, niin mahdollisten hyökkäysten kohteet ovat lisääntyneet. Vielä vähän aikaa sitten hyvin moni kotitietokoneen käyttäjistä ei tiennyt, mikä on anti-virus ohjelma tai palomuuri. Nykyään tilanne on huomattavasti parempi yleisen keskustelun ja tiedottamisen ansiosta. (Viestintävirasto 2004a.)

Monesti hyökkäykset eivät ole mitenkään tarkoin kohdistettuja, joten kohteena voi olla kuka tahansa, joka on kiinni koneineen Internetissä. Eli sen ajattelun, että eihän minun koneella ole mitään arvokasta tavoiteltavaa, voi unohtaa nykyaikana. Hyökkäysten tavoitteena onkin monesti tarkoitus saada vain kone hallintaan roskapostin lähetystä tai palvelunestohyökkäystä varten. (Viestintävirasto 2004a.)

Erilaisia hyökkäystapoja on monia ja se riippuu yleensä hyökkäyskohteesta ja hyökkääjän omista tavoitteista. Seuraavassa on kerrottu muutama tapa. Kohteen verkkotiedustelun (Host scanning) avulla hyökkääjä tutkii kohteen avoimia portteja ja kohteen käytössä olevia palveluja. Skannereilla voidaan tämä suorittaa automaattisesti, jolloin saadaan tutkittua tunnettuja tietoturva-aukkoja ja troijalaisten käyttämiä takaovia. (Viestintävirasto 2004b.)

Kohteen manipuloinnissa vedotaan suoraan ihmisten hyväntahtoisuuteen. Eli hyökkääjä pyytää esimerkiksi puhelimen tai sähköpostin avulla käyttäjätunnuksia ja salasanoja esimerkiksi jonkin ATK-ongelman korjaamiseksi. Toinen keino on naamioitua vaikka huoltomieheksi, jolloin on mahdollista yrittää päästä fyysisesti laitteiden lähelle. (Viestintävirasto 2004b.)

Salasanojen murtamiseen käytetään erillisiä ohjelmia, jotka yrittävät arvata käyttäjätunnus-salasanaparia. Murtamiseen käytetään yleisiä sanakirjoja, joiden sisältämiä sanoja ohjelmat käyvät läpi. Tämän takia salasanana ei kannata käyttää mitään erisnimiä tai mitään muuta valtakielessä perusmuodossa esiintyvää sanaa. (Viestintävirasto 2004b.)

Puskurin/syötteen ylivuodon tarkoituksena on ylittää sovelluksen syötetiedolle varaama tilavaraus, jolloin sovelluksen mahdollisen virhetilan myötä hyökkääjä pystyy antamaan komentoja järjestelmätasolla sovelluksen käyttöoikeuksilla. (Viestintävirasto 2004b.)

Hyökkäyksessä verkkoprotokollaa vastaan käytetään hyväksi verkkoprotokollan määrittelyissä olevia heikkouksia tai itse protokollan toteutuksen sisältämiä heikkouksia. Yksi suosituimmista palvelunestohyökkäyksistä on kuormitushyökkäys, jolla pyritään kuormittamaan kohdetta lähettämällä esim. suuren määrän palvelupyyntöjä lyhyessä ajassa. (Viestintävirasto 2004b.)

Haittaohjelmilla pyritään vaikuttamaan koneen omiin tietoturvaominaisuuksiin ja kiertämään ne, lisäksi avataan hyökkääjälle reitti järjestelmään sisältä päin hyökkäystä varten. Haittaohjelmat asentuvat usein toisen ohjelman välityksellä, sähköpostien liitteiden tai www-sivujen kautta. (Viestintävirasto 2004b.)

Domainin kaappauksessa pyritään vaikuttamaan nimipalvelimen toimintaan siten, että määrätylle domainille tarkoitetut palvelupyynnöt ohjautuvatkin hyökkääjän haluamaan paikkaan. Samantyylistä tapaa käytetään myös reitityksen väärentämisessä, jolloin hyökkääjä pystyy muuttamaan verkkoliikennettä siten, että tiettyyn osoitteeseen tarkoitetut paketit ohjautuvatkin hyökkääjälle. Tällöin hyökkääjä pääsee väärentämään, salakuuntelemaan tai tuhoamaan kahden laitteen välistä liikennettä. Lähdeosoitteen väärentämisessä hyökkääjä pyrkii väärentämään lähdeosoitteen, jotta hyökkäyksen kohde luulee pakettien tulevan turvallisesta osoitteesta. (Viestintävirasto 2004b.)

Rootkitit ovat olleet olemassa jo pitkään, vaikka ne ovat vasta nyt nousseet suuremman yleisön tietoisuuteen. Ensimmäiset havainnot rootkiteistä tehtiin noin kymmenen vuotta sitten Unix-ympäristössä. Rootkitin avulla yritetään esimerkiksi varastaa tietoja, käynnistää palvelunestohyökkäys tai piilottaa omat aikaansaannokset. Rootkit pystyy piilottamaan itsensä ja hyökkääjän muokkaamalla käyttöjärjestelmää ja korvaamalla perustoimintoja. Rootkitin avulla voidaan myös piilottaa muita haittaohjelmia. Koska rootkitin löytäminen ja poistaminen on työlästä, niin paras keino niitä vastaan on ennaltaehkäisy. Eli käytössä olisi hyvä olla tietoliikenneporttien käyttöä valvova palomuuri ja jokin ohjelma, jolla voidaan havaita haittaohjelmat. Järjestelmänvalvojan käyttäjätunnus ja salasana tulisi myös pitää hyvässä tallessa. Ohjelmia ei suositella asennettavaksi ja ajettavaksi järjestelmänvalvojan tunnuksilla. (Panda Software Finland, Rootkit ohjelmat 2005.)

Seuraavissa taulukoissa luetellaan SANS (SysAdmin, Audit, Network, Security) instituten listaamat 10 suurinta Internet-tietoturvauhkaa windows- ja unix-järjestelmille. Käytettävän tunkeutumisen havaitsemisjärjestelmien hälytystiedoissa tulee varmasti näkymään juuri näiden lueteltujen uhkien hyväksikäyttöyrityksiä. SANS päivittää tarpeen mukaan top-listojen tietoja uusien uhkien ilmaantuessa tai jos vanhoja uhkia koskevia uusia tietoja ilmaantuu.

Taulukko 1. Windowsin top 10 tietoturvauhat (SANS Institute, 2004)

Windows top 10 uhat
1. Web-palvelimet
2. Työasemapalvelut
3. Windows etäkäyttö
4. Microsoft SQL Server
5. Windowsin käyttäjäntunnistus
6. Nettiselaimet
7. Tiedostojen jako (p2p)
8. LSAS
9. Sähköpostiohjelmat
10. Pikaviestipalvelut

Taulukko 2. Linuxin top 10 tietoturvauhat (SANS Institute, 2004)

Linux top 10 uhat
1. BIND DNS
2. Web-palvelimet
3. Tunnistus
4. Versionhallintajärjestelmät
5. Sähköpostin siirtopalvelut SMTP
6. SNMP
7. OpenSSL
8. Väärin konfiguroitu NIS/NFS
9. Tietokannat
10. Ydin (kernel)

4. IDS

4.1 IDS:n historia

Ensimmäinen käsitys tunkeutumisen havaitsemisjärjestelmistä syntyi vuonna 1980 James Andersonin kirjoittaman tutkielman myötä. Se käsitteli tietoturvauhkien tarkkailua ja valvontaa. Tutkielma esitteli näkemyksen, että kirjausketju sisältää tunkeutumisen havaitsemiselle tärkeitä tietoja. Nämä tiedot auttaisivat havaitsemaan väärinkäytökset ja tietyn käyttäjän aiheuttamat tapahtumat. Tämä antoi alkusysäyksen laitekohtaisten IDS-järjestelmien ja yleensä IDS-järjestelmien kehitykselle. (The Evolution of Intrusion Detection Systems 2001.)

Vuonna 1983 SRI International ja erityisesti Dorothy Denning, aloitti hallituksen projektin. Tämän tavoitteena oli analysoida valtion hallinnon keskustietokoneen kirjausketjua ja luoda profiileja käyttäjistä heidän toimintojen pohjalta. (The Evolution of Intrusion Detection Systems 2001.)

Siitä syntyi IDES (Intrusion Detection Expert System), jonka ensimmäinen prototyyppi todisti, että poikkeamat käyttäjän normaalissa toiminnassa voidaan havaita reaaliajassa. IDES-ohjelman kehittymisen myötä SRI suoritti esitutkimusta FBI:lle IDES:in toteuttamisesta heidän maanlaajuiseen FOIMS-tietojärjestelmään. IDES for FOIMS-ohjelmaa ei kuitenkaan koskaan käytetty kuin testiolosuhteissa. (history of Intrusion Detection at SRI 2005.)

Rob Clyde oli vuonna 1980 perustamassa Clyde Digital Systems nimistä yritystä, joka teki ensimmäisen kaupallisen tunkeutumisen havaitsemisjärjestelmän Audit for VMS, joka sai myöhemmin nimen Intruder Alert. (Neohapsis / Archives / IDS List / Message Index / RE: IDS: RE: Info needed to compare Axent ITA and ISS RealSecure 2000.)

Lawrence Livermore Labs:in Haystack-projekti tuotti Yhdysvaltojen ilmavoimille vuonna 1988 tunkeutumisen havaitsemisjärjestelmän, joka analysoi tietoja

vertaamalla niitä ennalta määriteltyihin kuvioihin. Vuonna 1989 Haystack-projektin kehittäjät perustivat Haystack lab-yrityksen ja julkaisivat Stalker-nimisen tuotteen. Stalker oli konekohtainen, ja sen toiminta perustui edellä mainittuun kuvioiden tutkimiseen. Lisäksi siinä oli vankat hakumahdollisuudet joko manuaaliseen tai automaattiseen kyselyyn tiedoista. (The Evolution of Intrusion Detection Systems 2001.)

Ensimmäinen idea verkkopohjaisesta IDS:tä esiteltiin vuonna 1990 Todd Heberleinin toimesta. Järjestelmä oli nimeltään Network Security Monitor (NSM). NSM asennettiin valtion hallinnon järjestelmiin, joissa verkkoanalyysit tuottivat suuria määriä informaatiota. Heberleinin ja Haystack-tiimin saavutusten jälkeen esiteltiin idea hybridi IDS:stä, jossa on yhdistetty verkko- ja laite-IDS-laitteiden hallinta ja hälytykset. (The Evolution of Intrusion Detection Systems 2001.)

IDS:ien kaupallinen kehitys alkoi 1990-luvun alussa. Haystack labs:in Stalker oli ensimmäinen kaupallinen IDS. Science Applications International Corporation (SAIC) kehitti myös omaa host-IDS:ää nimeltään Computer Misuse Detection System (CMDS). (The Evolution of Intrusion Detection Systems 2001.)

Yhdysvaltojen ilmavoimien oma tunkeutumisen havaitsemisjärjestelmä, nimeltään Automated Security Measurement System (ASIM), selvitti ongelmat koskien skaalautuvuutta ja siirrettävyyttä. ASIM oli myös ensimmäinen tuote, joka sisälsi laitteiston ja ohjelmiston samassa. ASIM on edelleen tänä päivänä käytössä Yhdysvaltojen ilmavoimilla. ASIM:in kehittänyt ryhmä perusti vuonna 1994 oman yrityksen, Wheel Groupin, jonka NetRanger oli ensimmäinen kaupallisesti kannattava IDS-tuote. (The Evolution of Intrusion Detection Systems 2001.)

Vuonna 1997 alkoivat IDS-tuotteet tehdä voittoa yrityksilleen. Sinä vuonna ISS toi markkinoille oman tuotteensa, RealSecuren. Seuraavana vuonna Cisco osti Wheel Groupin, kun he ymmärsivät tunkeutumisen havaitsemisjärjestelmän tarpeellisuuden. (The Evolution of Intrusion Detection Systems 2001.)

4.2 Verkko IDS

Verkko-IDS eli NIDS valvoo koko verkkosegmenttiä tai aliverkkoa. Tämä saadaan aikaiseksi vaihtamalla verkkokortin toimintatapaa. Normaalisti verkkokortti kuuntelee vain paketteja, jotka ovat osoitettu sen omaan MAC-osoitteeseen. Muita paketteja ei tallenneta muistiin analysointia varten, vaan ne hylätään. Tässä toisessa toimintatavassa verkkokortti hyväksyy kaikki paketit ja tallentaa ne analysointia varten. (Beale, Caswell 2004, 10-12.)

Verkko-IDS:n hyvistä puolista yksi on se, että se ei vaikuta mitenkään tutkittavaan järjestelmään ja verkkoon. Lisäksi se ei aiheuta mitään kuormaa käyttäjille, ja hyökkäyksen yrittäjät eivät pääse käsiksi siihen, ja mahdollisesti verkko-IDS ei edes näy muille. (Beale, Caswell 2004, 10-12.)

4.3 Laitekohtainen IDS

Laitekohtainen-IDS eli HIDS valvoo vain sitä järjestelmää, jossa se sijaitsee, ei koko omaa aliverkkoa. Lisäksi verkkokortti toimii Verkko-IDS:stä poiketen normaalissa tilassa eli vastaanottaa vain koneelle tulevat paketit. Lisäksi säännöt tehdään vain tätä yhtä konetta ajatellen. Laitekohtainen-IDS pystyy havaitsemaan tarkoin määritellyt muutokset tiedostoissa ja käyttöjärjestelmässä. Laitekohtainen-IDS pystyy valvomaan tiedostojen kokoja ja tarkistussummia varmistaakseen, ettei tiedostoja muuteta huomaamatta. (Beale ym. 2004, 13-14.)

Laitekohtaisen-IDS:n valinnassa täytyy myös ottaa huomioon verkossa käytettävät käyttöjärjestelmät, jotta HIDS voidaan asentaa jokaiseen suojattavaan järjestelmään. HIDS aiheuttaa myös kuormaa laitteelle, ja tämä kannattaa ottaa huomioon varsinkin ruuhkaisessa serverikoneessa. On myös muistettava hyvin suunniteltu keskitetty hallinta. (Beale ym. 2004, 13-14.)

4.4 Hybridi IDS, DIDS ja honeypot

Hybridi-IDS:ssä on yhdistettynä laitekohtainen-IDS ja verkko-IDS. Hybridi-IDS eroaa kuitenkin verkko-IDS:stä sen verran, että se ei tarkista jokaista verkossa liikkuvaa pakettia. Hybridi-IDS on järjestelmäpohjainen, ja se tunnistaa hyökkäykset verkkopaketeista, jotka tulevat tai lähtevät yhdestä isännästä. Tällä vältetään ylikuormituksen aiheuttamat ongelmat. (Mitä on tunkeutumisenhavaitseminen? 2005.)

DIDS (distributed) eli hajautettu-IDS rakentuu erillisistä NIDS ja HIDS sensoreista, jotka raportoivat samaan järjestelmään. Hyökkäyslogit luodaan sensoreissa, joista ne ladataan keskusserverille, jossa ne tallennetaan keskustietokantaan. (Beale ym. 2004, 14-15.)

Honeypot eli ”hunajapurkki” on tietokone, jonka tarkoitus on tulla hyökätyksi. Tällä tavoin saadaan tietoa, todisteita ja jopa sijaintitietoa hyökkääjästä. Honeynet on taas joukko honeypot-koneita, kaksi tai useampi. (Andrés, Kenyon, Cohn, Johnson, Dolly 2004, 410.)

Hunajapurkkeja voi olla kahdenlaisia. Se voi olla laite, jossa palvelut ja palvelimet ovat simuloituja. Esimerkiksi Honeyd:llä voidaan simuloida tuhansia virtuaali hosteja yhtä aikaa. Lisäksi Honeyd pystyy simuloimaan erilaisia reititys topologioita ja eri käyttöjärjestelmiä. Tai vaihtoehtoisesti honeypot voi olla kone, johon on asennettu esim. oikea FTP tai Web-palvelin, joka on kuitenkin erotettu ja suojattu muusta verkosta erilleen. Lisäksi palvelimen sisältämien tietojen on tarkoitus näyttää hyökkääjän kannalta kiinnostavalta. (Andrés, Kenyon, Cohn, Johnson, Dolly 2004, 410,413.)

4.5 Tunkeutumisen havaitseminen

Tunkeutumiset voidaan havaita eri tavoilla, kolme yleisintä ovat sääntöpohjainen havaitseminen, protokollapoikkeavuuksien havaitseminen ja toiminnan poikkeavuuksien havaitseminen. (Mitä on tunkeutumisenhavaitseminen? 2005.)

Sääntöpohjainen havaitseminen on eniten käytetty havaitsemistapa. Tällöin etsitään liikenteen joukosta tiettyjä hyökkäyksen tuntomerkkejä. Hyökkäys pitää olla tunnettu, jotta sen havaitsemiseksi on voitu kirjoittaa oma sääntö. Tätä samaa ideaa käyttävät myös virustorjuntaohjelmat. (Mitä on tunkeutumisenhavaitseminen? 2005.)

Protokollapoikkeavuuksien havaitseminen tapahtuu havainnoimalla liikenteen rakennetta ja sisältöä, ja se tapahtuu sovellusprotokollatasolla. Sillä tavoin on mahdollista havaita hyökkäykset, jotka kohdistuvat esim. RPC-, SMTP- ,Rlogin-, HTTP- ja Telnet-protokollia vastaan. Sensori tunnistaa liikenteestä sille kerrotut sääntöjenvastaisuudet, kuten odottamaton data, ylimääräiset merkit ja kelpaamattomat merkit. (Mitä on tunkeutumisenhavaitseminen? 2005.)

Tässä havaitsemistavassa on yksi ongelma. Eli voi olla, että RFC-dokumenteissä eli Internetin erilaisia käytäntöjä kuvaavissa dokumenteissa jokin toiminta ei ole sallittua, mutta jonkin toimittajan ohjelmistossa samainen sovelluksen toiminta onkin täysin normaalia. Jolloin tuloksena on vääriä hälytyksiä, kuitenkin ohjelman toimiessa niin kuin sen kuuluukin. (Mitä on tunkeutumisenhavaitseminen? 2005.)

Toiminnan poikkeavuuksien havaitseminen tutkii tilastollisesti, mikä on normaalia ja mikä epänormaalia toimintaa. Tällöin hälytyksen voi laukaista esim. käyttö epätavallisina aikoina tai käyttäjäprosessien liikakäyttö. Tässä tavassa on hyvänä puolena se, ettei tarvitse ymmärtää poikkeavuuksien syitä. Ongelmaksi muodostuu kuitenkin se, että normaalikäytössäkin syntyy usein poikkeavuuksia, jolloin syntyy vääriä hälytyksiä. Tämä havaitsemistapa on näistä kolmesta vähiten käytetty. (Mitä on tunkeutumisenhavaitseminen? 2005.)

5. KAUPALLISET IDS:T

5.1 ISS Realsecure

ISS:ltä löytyy ohjelmistopohjaisia tunkeutumisen havaitsemisjärjestelmiä 10/100/1000 Mbps verkkoihin. RealSecuresta löytyy myös tarvittavat vastatoimet hyökkäysten torjumiseen. Realsecuresta löytyy NIDS ja HIDS-ominaisuudet. Realsecure on mahdollista asentaa Windows, Solaris ja Linux-järjestelmiin. Havaitseminen perustuu protokolla-analyysiin ja sääntöpohjaiseen havaitsemiseen. Hyökkäyksistä Realsecure tunnistaa muun muassa palvelunestohyökkäykset (WinNuke SYN Flood ja LAND), luvattomat sisäänpääsy-yritykset (Back Orifice ja Brute Force), ennen varsinaista hyökkäystä tapahtuvat tunnustelut (SATAN skannaus ja yhteydenotot käyttämättömiin palveluihin), epäilyttävät toiminnat (TFTP), yritykset asentaa takaovi-ohjelma (rootkit, BackOrifice2000), yritykset muuttaa tietoja tai sisältöä ja yritykset pysäyttää ja tappaa käynnissä oleva ohjelma. (RealSecure Network 10/100 FAQ 2003.)

ISS:ltä löytyy myös Proventia-nimisiä valmiita rautapohjaisia tunkeutumisen havaitsemisjärjestelmiä. Niiden nopeudet yltävät 200 -> 1200 Mbps yhteyksiin. (Proventia Intrusion Detection Appliances Datasheet 2003.)

Yhden 10/100 Mbps verkkoon tarkoitetun verkkosensorin hinta on noin 10000 € + vuotuiset ylläpitokustannukset ja gigabitin verkkoon tarkoitettu verkkosensori maksaa noin 30000 € + ylläpitokustannukset. Lisäksi tarvitaan hallinnointiohjelmisto, joitten hintahaitari on 5000-25000 €, riippuen siitä, kuinka kattavat toiminnot tarvitaan. (Internet security – iss datenblaetter 2005.)

5.2 Cisco IDS

Ciscolla on tarjota tunkeutumisen havaitsemiseen/estoon Cisco IPS 4200-sarjan laitteita, jotka auttavat havaitsemaan, luokittelemaan ja estämään uhat. Näitä uhkia ovat esimerkiksi madot, vakoilu/mainosohjelmat, verkkovirukset ja ohjelmien väärinkäyttö. (Cisco IPS 4200 Series Sensors 2006.)

Ciscolla on myös integroitava IDS-moduuli nimeltään IDSM-2, joka voidaan yhdistää Catalyst 6500 ja 7600 laitteisiin. IDSM-2 voi toimia joko tunkeutumisen esto- tai tunkeutumisen havaitsemislaitteena. Ollessaan passiivitilassa eli suorittaessaan vain havainnointia sen suorituskyky riittää 600 Mbps liikennemäärään 450 tavun paketeilla, ja uusia TCP-yhteyksiä ja http-tapahtumia se pystyy käsittelemään 6000 kpl/sekunnissa. Aktiivi eli tunkeutumisen estotilassa liikennemäärä voi olla 500 Mbps 450 tavun paketeilla, ja uusia TCP-yhteyksiä ja http-tapahtumia se pystyy käsittelemään 5000 kpl/sekunnissa. (Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Service Module 2006.)

4200-sarjan laitteista sain suomalaiselta jälleenmyyjältä tietoa hinnoista sen verran että Cisco IDS 4215 sensor, joka suoriutuu tarkasti 65 Mbps liikenteestä ja on tarkoitettu pienille ja keskisuurille yrityksille maksaa 4415 €, Ciscon IPS 4240 Appliance Sensor, joka pystyy maksimissaan 250 Mbps liikenteeseen maksaa 7259 €, IPS 4255 Appliance Sensor ,joka pystyy 500 Mbps liikenteen seuraamiseen maksaa 15126 € ja 4250 Sensor, joka pystyy 800 Mbps liikenteen seuraamiseen maksaa 16339 €. Kaikki hinnat ovat alv 0%. Nämä hinnat kertovat ainakin suunnan, missä luokassa näiden laitteiden hinnat ovat. Lisäksi myös näihin hintoihin tulee päälle ylläpitokustannukset, jotka riippuvat vasteajoista.

5.3 NFR sentivist ids/ips

NFR Security tarjoaa rautapohjaista Sentivist-tunkeutumisen havaitsemisjärjestelmää, josta löytyy myös tunkeutumisen esto-ominaisuudet. Sentivist pystyy valvomaan verkkoa nopeusluokissa 10/100/1000 Mbps. Sentivist-

havaitseminen perustuu pääosin sääntöpohjaiseen havaitsemiseen ja protokollapoikkeavuuksien havaitsemiseen. Sentivististä on kolme eri mallia olemassa 320C, 320F ja 310C. 320C sisältää kolme 10/100/1000 Mbps ethetnet kupariliitäntää, joista yksi on tarkoitettu hallintaa varten ja kaksi havainnointia varten. 320F sisältää kaksi 10/100/1000 Mbps ethernet-kupariliitäntää ja kaksi gigabitin ethernet-valokuituliitäntää, joista yhtä kupariliitäntää käytetään hallintaan ja muita havainnointia varten. 310C sisältää kaksi 10/100/1000 Mbps ethernet-kupariliitäntää, joista toinen on hallintaa varten ja toinen havainnointia varten. Sentivist tarvitsee myös erillisen serveri-koneen, jota tarvitaan useiden sensoreiden hallintaan sekä hälytys- ja muun datan tallennustilaksi. Vähimmäisvaatimuksena serverille on tupla-prosessori pentium, joka toimii vähintään 1,4Ghz kellotaajuudella, ja keskusmuistia tulisi olla vähintään 2 Gt. Myös kaksi 40 Gt SCSI-kovalevyä, jossa on Raid 0+1, 1 tai 5 konfiguraatio. Sentivist-sensorista on olemassa myös ohjelmallinen versio. (NFR Sentivist version 4 2004.)

5.4 Enterasys Dragon

Enterasysilta on tarjolla Dragon-niminen tunkeutumisen havaitsemis- ja estojärjestelmä windows, linux, solaris ja HP-UX-käyttöjärjestelmiin. Dragon toimii sekä NIDS- että HIDS-laitteena. Havainnointi tapahtuu tutkimalla toiminnan poikkeavuuksia, valvomalla protokollien poikkeavuuksia ja sääntöpohjaisella havaitsemisella. Dragon-laitteita on neljää eri mallia FE100, GE250, GE500 ja GIG Dragon Network Sensor Appliance. Mallien nimet kertovat, minkänopeuksiseen verkkoon laite on tarkoitettu, eli FE100 on tarkoitettu 100 Mbps verkkoon, ja GIG on tarkoitettu 1 Gbps verkkoon. Keskusmuistia laitteissa on 1Gb, paitsi GIG:ssä on 2 Gb. Suorittimina laitteissa käytetään lähtien FE100-laitteen Intel Celeronista päättyen GE500 ja GIG-mallien tupla Intel Xeon-ratkaisuihin. (Dragon 7 network intrusion detection and prevention 2006.)

5.5 Symantec Network Security

Network Security löytyy sekä ohjelmisto- että rautapohjaisena IDS-tuotteena, jossa on myös IPS. Se vaatii alustakseen Linuxin tai Solariksen. Network Security pystyy 2 Gbps nopeuksiin havainnoinnissa, ja havaitsee hyökkäykset sääntöpohjaisella ja protokollapoikkeavuuksien havaitsemisella. (Symantec Network Security data sheet 2004.)

Symantecin Network Security 7100-mallisto sisältää kolme laitetta 200 Mbps nopeudesta aina 2Gbps nopeuksiseen laitteeseen asti. (Symantec Network Security 7100 series 2005.)

Taulukko 3. Symantec Network Security 7100-mallisto (Symantec Network Security 7100 series 2005.)

Malli	7120	7160	7161
IDS kapasiteetti	200 Mbps	2 Gbps	2 Gbps
IPS kapasiteetti	100 Mbps	1 Gbps	1 Gbps
Yhteyksiä/sekunnissa	1500	12,500	12,500
Verkkoliitännät	4 kpl 10/100 kupariliitäntää	8 kpl 10/100/1000 kupariliitäntää	4 kpl 10/100/1000 kupariliitäntää ja 4 kpl 1000 Base-SX valokuituliitäntää

SC-magazine testasi kaupallisia IPS-laitteita vuonna 2005. Symantecilta mukana oli 7120-malli, joka pärjäsi kohtalaisesti testissä saaden kolme tähteä viidestä maksimista. Java-pohjaista hallintakonsolia kiiteltiin helppokäyttöisyydestä, vaikka se saattaakin aluksi vaikuttaa sekavalta. Laitteesta puuttuu myös jotain huippuominaisuuksia, mutta hinta-laatusuhde on hyvä. Huonoa on IDS- ja IPS-

tilojen välinen nopeusero eli IDS-tilassa kapasiteetti on 200 Mbps ja IPS-tilassa 100 Mbps. (Product reviews – SC magazine US Symantec Network Security 2005.)

5.6 Sourcefire

Sourcefire on Snortin kehittäjän Martin Roeschin vuonna 2001 perustama yritys, joka valmistaa rautapohjaisia Tunkeutumisen havaitsemis/estolaitteita. Sourcefire käyttää Snortia laitteidensa perustana ja parhaimmat laitteet tukee nopeuksia aina 8 Gbps asti. Snort on itsessään maailman levinnein tunkeutumisen havaitsemis tekniikka ja sitä pidetään tällä hetkellä käytännön standardina IDS-maailmassa. Havaitsemisessa tukeudutaan sääntöpohjaiseen, protokollapoikkeavuuksien ja toiminnan poikkeavuuksien havaitsemiseen. (Sourcefire Network Security – Intrusion Sensor 2005.)

SC-magazinen testissä Sourcefiren IPS-laite oli testivoittaja saaden täydet 5 tähteä. Sensori on Intel-pohjainen laite, jossa on Linux-käyttöjärjestelmä, jonka tietoturvatasoa on nostettu korkeammaksi. Hallinta hoidetaan nettiselaimen avulla ja on hieman vaikeakäyttöinen. Ominaisuuksia laitteesta kuitenkin löytyy paljon ja yksi tärkeimmistä on kyky havaita 0-päivän hyökkäykset, eli hyökkäykset, jotka alkavat samana päivänä, kuin haavoittuvuus on löydetty. Pelkkä sensori ei ole parhaimmillaan itsenäisenä laitteena, kuten muut IPS-laitteet tässä testissä ovat. Sourcefiren 3D-system-järjestelmä koostuu useasta eri laitteesta. 3D tulee englanninkielen sanoista discover, determine ja defend eli havaitse, päätä, ja puolusta. 3D-System on kuitenkin kattavin järjestelmä, joka on markkinoilla ja joka sopii parhaiten suuriin verkkoihin monimutkaisuutensa ja korkean hintansakin vuoksi. (Product reviews – SC magazine US Sourcefire 3D System 2005.)

6. OPEN SOURCE IDS:T

6.1 Snort

Snort on verkko-IDS, joka perustuu avoimeen lähdekoodiin. Se suorittaa reaaliaikaista liikenneanalyysia ja pakettien kirjausta IP-verkoissa. Snort pystyy suorittamaan protokolla-analyysia ja sisällön vertailua ja tutkintaa, ja se havaitsee erilaisista hyökkäyksistä mm. puskurien ylivuodot, porttiskannaukset, käyttöjärjestelmähyökkäykset ja haittaohjelmien käytön esim. P2P-ohjelmat. Snort tarkistaa jokaisen verkossa kulkevan paketin, ja snortin säännöt määrittävät sen, kirjataanko paketti vai ei. (About Snort, 2005.)

Alun perin Snortin oli tarkoitus olla pakettisnifferi. Se julkaistiin joulukuussa 1998, ja ohjelma sisälsi silloin koodia 1600 riviä ja koostui kahdesta tiedostosta. Tammikuussa 1999 Snortin ominaisuuksiin lisättiin sääntöpohjainen analysointi, mistä lähtien sitä voitiin jo pitää kevyenä tunkeutumisen havaitsemisjärjestelmänä. Joulukuussa 1999 julkaistiin ohjelmasta 1.5 versio , ja siitä lähtien Snortissa oli mahdollista käyttää erilaisia plug-ineja. (Beale, Caswell, Foster, Posluns 2003, 29-30)

Versio 2.0 oli seuraava kulmakivi ohjelman kehityksessä, ja silloin Snort sisälsi jo 75000 riviä koodia. Mahdolliseksi tuli myös tietokantojen, kuten MySQL, MSSQL ja Postgres, käyttö. Lisäksi käytössä oli esikäsittelijä plug-init, jotka tutkivat paketit, ennen kuin ne menevät sääntöjen tutkittavaksi. (Beale ym. 2003, 30-31)

6.2 Shadow

Shadow on unix-järjestelmissä toimiva ilmaisohjelmisto, jonka Yhdysvaltojen laivaston pintasodankäynnin keskuksen Dahlgren-jaosto kehitti. Shadow koostuu kahdesta laitteesta, sensorista ja analysaattorista. Shadow eroaa muista NIDS-laitteista siten, että sen sensori tutkii paketeista vain otsikkotiedot, eikä näin ollen tutki ollenkaan paketin sisältämää tietosisältöä. Analysaattori tutkii sensorin

keräämät tiedot ja näyttää kiinnostavat tiedot www-sivuilla. Tulosten esitys tapahtuu Apache web-serverin kautta. Shadow ei ole myöskään tosiaikainen, vaan tulokset haetaan sensorilta ennalta määrätyn ajan välein analysaattorille. Shadowia on mahdollista käyttää yhdessä Snortin kanssa, jolloin saadaan yhdistettyä molempien vahvuudet. (Northcutt, Novak 2002, 248-249)

6.3 Bro

Bro on unix-järjestelmissä toimiva tunkeutumisen havaitsemisjärjestelmä. Se havaitsee tunkeutumiset vertaamalla liikennettä sen omiin sääntöihin. Säännöissä voidaan kuvailla hyökkäys tarkasti, tai sitten yleisemmin epätavanomaisia toimintoja. Bro:ssa on mahdollista käyttää myös Snortin sääntöjä, joskin ne pitää kääntää erillisen snort2bro scriptin avulla Bro:n ymmärtämään muotoon. Jos Bro havaitsee jotain kiinnostavaa, se voi merkitä tapahtuneen lokiin tai se voi suorittaa käyttöjärjestelmäkomennon. Bro luvataan pystyvän valvomaan Gbps-luokan verkkonopeuksia asennettuna täysin kaupasta saatavaan koneeseen. Bro:ta mainostetaan hyvin muunneltavana ja joustavana ohjelmana, joka on ehkä tarkoitettu enemmän asiantuntijoiden käyttöön kuin kotikäyttöön. Ja koska kyseessä on avoimen lähdekoodin tuote, niin sen tuotetuki ja yleinen ohjeistus on vajavaista. (Bro Intrusion Detection System 2005.)

7. ACTIVE RESPONSE JA INLINE-JÄRJESTELMÄT

7.1 SnortSam

Tässä esiteltävistä ohjelmista SnortSam voidaan luokitella active response-järjestelmäksi, kun taas kaksi jälkimmäistä ovat enemmän IPS-järjestelmiä. Active response tyyppiset järjestelmät pystyvät reagoimaan hyökkäyksiin vasta, kun hyökkäys on havaittu. SnortSamin toiminta perustuu vuorovaikutukseen palomuurin kanssa. Ohjelma ajetaan taustaprosessina palomuurikoneessa, ja se vastaanottaa komentoja Snortilta salatun TCP-yhteyden avulla. Näiden Snortilta saamiensa ohjeiden perusteella se estää IP-osoitteita liikennöimästä ja lisäksi voidaan määrittää, kuinka kauan kyseinen IP-osoite voidaan pitää estettynä. Snortsam on kuitenkin tässä esitellyistä ratkaisuista ainoa, joka on mahdollista saada näkymättömäksi hyökkääjälle. (Beale ym. 2004, 607-610.)

7.2 FwSnort

SnortSamsta poiketen fwSnort ei perustu active response -tekniikkaan, vaan on inline-järjestelmä. Inline-toiminnassa kaikki liikenne kulkee estojärjestelmän läpi, jolloin hyökkäykset voidaan estää saman tien. FwSnort-toiminta perustuu snortin sääntöihin ja iptablesiin. Fwsnort kääntää Snortin säännöt iptablesin käyttämään muotoon. Fwsnort ei pysty kuitenkaan kääntämään kaikkia snortin sisältämiä sääntöjä iptablesille. Snort 2.3- version säännöistä se kykenee kääntämään 54%. FwSnort olisi tarkoitus asentaa suoraan iptables palomuurin yhteyteen toimiakseen oikein (Beale ym. 2004, 609-610.)

7.3 Snort_inline

Snort_inline rakentuu pitkälti Snortin päälle lisäten siihen tunkeutumisen esto-ominaisuudet, eli muuttaa tai pudottaa kokonaan paketteja. Snort_inline on ollut saatavilla Snortn versiosta 2.3.0 eteenpäin. Myös snort_inline käyttää apunaan

iptablesia. Tarkemmin sanottuna Snort_inline ei saa paketteja libpcap:ltä vaan iptablesilta ja se käyttää hyväkseen Snortin säännöistä seuraavia toimintatapoja drop, reject ja sdrop. Niistä on lisää tietoa taulukossa 3. Snort_inline tulisi asentaa sillaksi kahden verkkosegmentin välille, jotta se toimisi. Honeynet project käyttää snort_inlinea tutkimustöissään. (Beale ym. 2004, 609-611.)

7.4 Tunkeutumisen estojärjestelmien hyvät ja huonot puolet

Hyvänä puolena voidaan mainita, että hyvin asennettu ja säädetty järjestelmä todellakin pystyy estämään ne hyökkäykset, jotka palomuurilta jää huomaamatta. Hyvänä puolena täytyy myös mainita SnortSam-ohjelmasta se, että johtuen sen active response luonteesta se saadaan näkymättömäksi hyökkääjiltä, joten itse laitteeseen ei suoraan voida hyökätä. Huonona puolena on se, että tunkeutumisen estojärjestelmää voidaan käyttää itse puolustettavaa verkkoa vastaan. Tämä tapahtuu niin että hyökkääjä väärentää hyökkäyksen lähdeosoitteeksi osoitteen, joka on ollut tähän asti täysin luotettava lähde, mutta tunkeutumisen estojärjestelmä tekee omat johtopäätökset ja estää liikenteen kyseisestä osoitteesta. Onneksi joissain tuotteissa on olemassa mahdollisuus määrittää, mitä liikennettä ei saa missään tapauksessa estää. (Beale ym. 2004, 607-610.)

8. SNORT

8.1 Snortin toiminta

Snortia käytettäessä NIDS:nä käyvät paketit seuraavanlaisen ketjun läpi. Ensin pakettidekooderi jäsentää paketit, jonka jälkeen paketit kulkevat esikäsittelijöiden läpi. Sen jälkeen data viedään sormenjälkitunnistukseen tunnistemoottorille, joka vertailee dataa käytössä oleviin sääntöihin. Esikäsittelijän ja tunnistemoottorin löytämät vastaavuudet viedään sitten erilaisiin tulosteisiin, joko lokeihin, tietokantaan tai suoraan näytölle. (Beale ym. 2004, 62-63.)

8.1.1 Pakettidekooderi

Kun paketit tulevat verkkokortille, niin sen jälkeen pakettidekooderi tulkitsee, mikä protokolla paketilla on käytössä. Sen jälkeen tietoja verrataan protokollan sallittuihin käyttäytymisnormeihin. Pakettidekooderi pystyy tekemään itse hälytyksiä viallisista protokollaotsikoista, liian pitkistä paketeista, ja epätavallisista tai vääristä TCP-optioista otsikkotiedoissa. Kun dekooderi on tulkinnut paketin, se lähetetään eteenpäin esikäsittelijöille. (Beale ym. 2004, 63-64.)

8.1.2 Esikäsittelijät

Esikäsittelijät ovat snortin plugineja, jotka osaavat jäsentää paketteja, jotta paketteja ei tuijotettaisi vain yksittäisinä paketteina. Monissa hyökkäyksissä käytetään hyväksi useita erillisiä paketteja, joihin hyökkäyksen käyttämät tiedot on laitettu. Perfmonitor on yksi hyödyllinen esikäsittelijä, ja sen tarkoituksena on kerätä tietoja Snortin suorituskyvystä. Snortin 2.4.0 versiosta löytyy 13 esikäsittelijää. (Beale ym. 2004, 64.)

Taulukko 3. Snortin esikäsittelijät (Snort manual 2.4)

ESIKÄSITTELIJÄ	TOIMINTA
Frag3	Kokoaa pirstoutuneita paketteja kohde ip:n perusteella
Stream4	Tarkoitettu TCP-tietovuon kokoamiseen.
Flow	Tarkoitettu Snortin tilojen yhdistämiseen yhteen paikkaan
Portscan	Vanhentunut flow-portscanin myötä
Flow-Portscan	Vanhentunut sfPortscanin myötä
sfPortscan	Tarkoitettu havaitsemaan esimerkiksi NMAP:lla tehdyt verkon skannaukset
Telnet Decode	Normalisoi Telnetin hallinta protokollan merkistön
Rpc Decode	Normalisoi pirstoutuneet RPC-tiedot yhdeksi tietueeksi
Performance monitor	Mittaa Snortin suorituskykyä
HTTP inspect	HTTP-dekooderi eli tulkitsin
ASN.1 detection	Etsii paketeista haitallisia koodauksia
X-link2State	Tarkoitettu huomaamaan X-link2State-haavoittuvuus Microsoft Exchange Serverissä
Frag2	Korvattu Frag3-esikäsittelijällä

8.1.3 Tunnistemoottori

Snortin tunnistemoottorin tehtävänä on vertailla pakettidekooderilta ja esikäsittelijältä tulevia tietoja snort.conf-tiedostossa mainittuihin sääntöihin.

Ensimmäisenä tunnistemoottori yrittää päättää, mikä säännöstö vastaisi kyseisiä tietoja. Luokittelu aloitetaan protokollasta, eli onko käytetty TCP-, UDP-, ICMP- vai IP-protokollaa, ja sen jälkeen tutkitaan protokollan ominaispiirteitä. TCP- ja UDP-protokollissa ominaispiirre on kohde- ja lähdeosoite, ICMP-protokollalle se on ICMP-tyyppi ja lopuille IP-paketeille se mitä muuta kuin TCP, UDP, ICMP-protokollaa käytetään tiedonsiirtoprotokollana. (Beale ym. 2004, 67.)

8.2 Snortin säännöt ja tunnistaminen

Aikaisemmin Snortin sääntöjä käytettiin sillä periaatteella, että järjestelmän löytäessä ensimmäisen vastaavuuden säännöistä paketin tietoihin Snort pystyi antamaan vain yhden hälytyksen. Monet muut IDS-järjestelmät pystyivät tuottamaan useamman hälytyksen samasta paketista. Nykyisin myös Snort on kykenevä tuottamaan useamman hälytyksen samasta paketista. (Beale ym. 2004, 67-68.)

Alkuun oli käytössä sellainen toiminto, että hälytys annettiin sen säännön mukaan, millä oli pisin vastaavuus paketin sisältöön, jos paketin sisältö vastasi useampaa sääntöä. Tämä antoi hyökkäyksille sen mahdollisuuden, että alettiin käyttää pakettien naamioimista, kun Snort huomasi paketin sisällöstä vain sen pidemmän vastaavuuden säännöissä eikä välttämättä huomattavasti vakavampaa sisältöä joka muodosti paketin sisällöstä vain pienen osan. Tämä ongelma ratkaistiin kahdella tavalla. Ensinnäkin Snort antaa hälytykset pisimmän vastaavuuden mukaan jokaisesta sääntöryhmästä erikseen eikä kaikkien sääntöjen joukosta. Toiseksi voidaan määrittää että hälytys annetaan ennemmin prioriteetin mukaan kuin pelkän suuremman paketin sisällön vastaavuuden vuoksi. (Beale ym. 2004, 68.)

Snortin säännöt koostuvat karkeasti ottaen kahdesta osasta: säännön otsikosta ja säännön optioista. Otsikko-osasta löytyy, kuinka säännön tulee toimia, protokollan tyyppi, lähde- ja kohde-ip-osoitteet, aliverkon peite ja lähde- ja kohdeportit. Säännön optio-osa sisältää viestin, mikä tulostetaan hälytyksen syntyessä ja tiedon siitä, mitä kohtaa paketista tulisi tutkia. Sääntöjen otsikkokohdasta löytyy siis tieto

siitä, kuinka Snortin tulee toimia, kun se löytää paketin, joka vastaa kaikkia säännön kriteerejä. Yhteensä eri toimintoja on kahdeksan, joista viittä käytetään Snortin normaalikäytössä ja loppuja kolmea käytetään silloin, kun Snortia käytetään tunkeutumisen estotarkoituksessa. Taulukossa 4 on esitelty sääntöjen eri toimintamallit. Ensimmäiset viisi ovat siis Snortin normaaleja toimintatapoja. (Snort users manual 2.4.0 RC1, 2006.)

Taulukko 4. Snort rule actions (Snort manual 2.4)

1. alert	Tekee hälytyksen ja kirjaa paketin
2. log	Kirjaa paketin
3. pass	Jättää paketin huomioimatta
4. activate	Tekee hälytyksen ja käynnistää dynaamisen säännön
5. dynamic	On toimeton kunnes activate-toiminto käynnistää sen ja toimii sen jälkeen samalla tavalla kuin log toiminto
6. drop	Saa iptablesin hylkäämään paketin ja kirjaa paketin
7. reject	Saa iptablesin hylkäämään paketin ja jos kyseessä on TCP paketti niin lähettää reset-paketin ja jos kyseessä on UDP paketti niin lähetetään kohde saavuttamaton ICMP viesti
8. sdrop	Saa iptablesin hylkäämään paketin mutta pakettia ei kirjata

```
alert udp ![192.168.xxx.xxx,193.166.xxx.xxx] 67 -> any
68 (msg: "Rogue DHCP server"; sid:1000002; priority:1;
classtype:misc-attack;)
```

Tässä esimerkkisäännössä näkee, että tavatessaan kyseistä liikennettä Snortin tulee tehdä hälytys ja kirjata paketti. Lähdetiedoissa määritellään, että hälytys tapahtuu, jos lähdeosoite ei ole kumpikaan mainituista ja lähdeportin tulee olla 67. Kohde osoite saa olla mikä tahansa, mutta kohdeportin tulee olla 68. Msg-kohtaan voi kirjoittaa sen, mikä itsellesi parhaiten kuvaa hälytystä. Sid-numerolla yksilöidään jokainen sääntö, ja tätä tietoa käyttävät tulostus-pluginit, yli miljoonan menevät luvut ovat varattu itse kirjoitetuille säännöille. Snortin viralliset säännöt käyttää numeroita 100-1000000. Bleeding snort-säännöt käyttävät yleisesti yli kahden miljoonan meneviä numeroita. Priority on tässä tapauksessa korkein eli 1.

Classtype eli sääntöjen luokittelun voi tehdä myös oman mielesi mukaan. On myös huomattava, että jokaisella hälytysluokalla on oletusprioriteetti, joka on hyvä tarkastaa snortin manuaalista, kun kirjoittaa omia sääntöjä. Prioriteettitasoja on kolme 1-3, korkeasta matalaan.

8.3 Muut snortin käyttöön liittyvät ohjelmat

8.3.1 oinkmaster

Oinkmaster on perl-kielellä tehty melko yksinkertainen ohjelma, jolla voidaan päivittää Snortin säännöt äärimmäisen helposti. Se toimii useimpien Unix-käyttöjärjestelmien kanssa ja myös Windows-käyttöjärjestelmissä, mutta silloin tarvitaan lisäksi Cygwin tai ActivePerl-ohjelma. Oinkmasterin avulla voi päivittää säännöt joko Snortin virallisilla lisensoiduilla säännöillä, Snortin yhteisösäännöillä tai jonkin ulkopuolisen tekijän, kuten Bleeding Snortin säännöillä. Mahdollisuus on myös ladata sääntöjä monesta eri paikasta samalla kertaa. Ohjelmalla voi myös määritellä ne säännöt, joita ei haluta päivittää. Oinkmasteriin on olemassa graafinen käyttöliittymä, joka vaatii vielä tekijöiden mielestä testausta. (Oinkmaster features, 2005.)

8.3.2 BASE

BASE eli Basic Analysis and Security Engine on web-käyttöliittymä, jolla voi kätevästi tehdä kyselyitä ja tutkia Snortin hälytystietokantaa. BASE perustuu ACID-nimisen projektin koodiin, ja ACID oli BASE:n ilmestymiseen asti se ohjelma, jota yleisesti neuvottiin kirjoissa ja muissa dokumenteissa käyttämään Snortin yhteydessä. (Basic Analysis and Security Engine (BASE) project, 2004.)

BASE:n suosio perustuu myös varmasti sen helppokäyttöisyyteen ja helppoon asennettavuuteen. Ja jos haluaa käyttää Snortin kanssa arkistotietokantaa, niin

BASE:lla onnistuu myös sen hallinta. Runsaiden hakuominaisuuksien avulla voidaan arkistoida halutut hälytykset helposti muutamalla hiiren näpäytyksellä.

8.3.3 Archiveplus

Archiveplus on perl-kielellä kirjoitettu pieni ohjelma, jonka avulla on mahdollista siirtää tai kopioida kätevästi hälytyksiä varsinaisesta snort-tietokannasta arkistotietokantaan jos sellaista käyttää. Archiveplus tukee tällä hetkellä vain MySQL-tietokantojen arkistointia, joskin se taitaa olla tällä hetkellä käytetyin tietokanta Snortin kanssa. Cronin avulla scripti on helppo suorittaa vaikka keskellä yötä, jolloin se hoituu huomaamattomasti joka päivä. Erilliseen asetustiedostoon määritellään, kuinka monta vuorokautta vanhat hälytykset kopioidaan/siirretään arkistotietokantaan. Päätietokantaa varten käyttäjä tarvitsee select, delete ja file-oikeudet ja arkistotietokantaa varten select, insert ja file oikeudet. Nämä annetaan MySQL:ssä esimerkiksi seuraavalla tavalla.

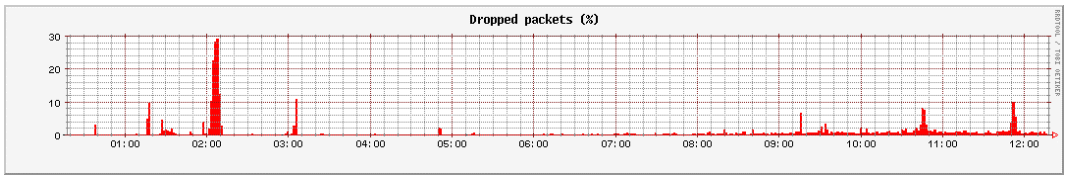
```
mysql> grant SELECT on root.* to snort@localhost;
```

8.3.4 Barnyard

Verkkojen nopeuksien kasvaessa huomattiin, että Snortilla oli vaikeuksia kirjata kaikkia verkossa liikkuvia paketteja. Syy tähän oli se että tietojen vieminen SQL-tietokantaan oli suhteellisen hidas prosessi. Ja koska Snort ei tue monisäikeisyyttä, voi ruuhkaisena aikana jäädä paketteja kirjaamatta SQL-toimintojen vuoksi. Snortiin tehtiin laajennus, jolla voidaan välttää Snortin kirjoittaminen suoraan SQL-tietokantaan, tiedot kirjoitetaan erilliseen binäärimuotoiseen tiedostoon. Tässä vaiheessa tulee mukaan Barnyard, joka voi viedä tiedot SQL-tietokantaan, luoda CSV-muotoisia tiedostoja tai luoda syslog-ilmoituksia. (Beale ym. 2004, 530-531.)

8.3.5 Perfmonitor-graph

Perfmonitor-graph on pieni perl-kielellä kirjoitettu ohjelma, joka luo HTML-sivun, jossa on graafisessa muodossa Snortin perfmonitor esikäsittelijän tulosteita. Perfmonitor-graph käyttää kuvien luomiseen RRD-tool ohjelmaa. Kuvista näkee nopeasti, jos Snortilla on ollut jotain ongelmia esimerkiksi suorituskyvyssä, jos seuraa kuviossa 3 näkyvää pudotettujen pakettien määrää ja suorittimen käyttöastetta. Muita hyödyllisiä kuvioita ovat hälytysten määrä sekunnissa, liikenteen määrä Mbit/sekunnissa, kuinka monta tuhatta pakettia liikkuu sekunnissa, SYN ja SYN+ACK pakettien määrä sekunnissa ja pakettien keskimääräinen koko. (Perfmon-graph 2006.)



Kuvio 3. Perfmonitor-graph pudotetut paketit

8.3.6 Snort Report 1.3.1

Snort Report 1.3.1 on Snortin lisäosa, jonka tarkoituksena on tuottaa tosiaikaisia raportteja Snortin tietokannasta. Ohjelma toimii niissä käyttöjärjestelmissä, joissa saadaan Apache ja PHP toimimaan. Ohjelma on saatu toimimaan Linuxissa, Macin OSX:ssä ja Windowsissa. Tietokannoista Snort Report 1.3.1 tukee MySQL 4.x versioita ja PostgreSQL:ää. MySQL:n aikaisempia ja myöhempiä versioita ei ole testattu, mutta myös niiden pitäisi toimia. Snortista suositellaan käytettäväksi 2.4-versiota. Jos raporttiin halutaan mukaan graafisia kuvaajia niin pitää asentaa GD-kirjasto ja Jpgraph. Snort Report-ohjelmasta on esimerkkinäkymä liitteessä 2, jossa näkyy yhteenvetoa Snortin hälytyksistä, ja lähinnä eniten tapahtuneet korkeimman prioriteetin hälytykset. (Snort Report FAQ, 2005)

9. TUNKEUTUMISEN HAVAITSEMISJÄRJESTELMÄN KÄYTTÖÖNOTTO

9.1 Snortin asennus

Snortin asennus jouduttiin tekemään hieman alitehoiseen testikoneeseen, kun muuta konetta ei ollut asennushetkellä saatavissa. Samaista konetta on käytetty myös aikaisemmin Snortia testatessa. Ja vaikka kone välillä hidastelee ja liikennettä jää joskus näkemättä tehonpuutteen vuoksi, niin ohjelman ominaisuudet on hyvin tullut havaittua.

Snortia varten koneeseen asennettiin käyttöjärjestelmäksi Fedora Core 3, joka toiminut pienten alkuvaikeuksien jälkeen ongelmattomasti. Alkuvaikeudetkin johtuivat enemmän käyttäjästä kuin käyttöjärjestelmästä. Asennusohjeena käytin jo aiemmin hyväksi havaittua opasta joka löytyy osoitteesta http://www.internetsecurityguru.com. Tässä asennuksessa käytin ohjeesta versiota, joka on kirjoitettu 24.10.2005. Koko ohje on liitteessä 3.

Asennuksen alku menee ohjeiden mukaan paitsi, että valitsin näppäimistön kieleksi suomalaisen, kun siihen olen tottunut. Ja seuraavaksi tietysti valittiin mukautettu asennustyyppi, jotta voidaan valita sopivan kevyt asennus. Levyn osiointi tapahtui automaattisesti tähän kokoonpanoon. Käynnistysohjelma ja käynnistysoptiot jätettiin oletusvaihtoehdoiksi. Käyttöjärjestelmää asentaessa koneessa oli vain yksi verkkokortti ja konfiguroin sen ip-asetukset käsin. Palomuuri laitettiin päälle ja palveluista otettiin mukaan SSH, HTTP ja HTTPS. SSH on hyvä olla sallittuna, kun otetaan koneeseen pääteyhteys esim. Putty-ohjelmalla. HTTP ja HTTPS sallittiin, jotta voitiin käyttää www-palvelin ominaisuuksia. SELinuxin otin pois päältä, koska sen kanssa oli jotain ongelmia aikaisemman Snortin asennuksen kanssa. Ja aikavyöhykkeeksi tuli tietenkin Suomi.

Seuraavaksi tulee käsittelyyn ehkä se tärkein asennuksen vaihe, eli mitä paketteja asennetaan. Aikaisempi Internet Security Gurun asennusohje suositteli asennettavaksi graafista käyttöliittymää, mutta uusin versio ei sitä enää neuvo. Itse

olen asiasta samaa mieltä, koska Snortin ohjaaminen tapahtuu täysin komentotulkin kautta ja tarvetta graafiseen ympäristöön ei ole. Ja tehoa ei mene turhaan graafisen ympäristön ajamiseen varsinkin jos ei ole viimeisintä mallia oleva kone. Mukaan asennukseen otettiin ohjeen mukaan editorit, mutta poistettiin tekstipohjainen Internet ja loput paketeista valittiin ohjeen mukaan.

Uudelleenkäynnistyksen jälkeen luotiin käyttäjäryhmä, käyttäjä ja käyttäjälle salasana. Ohjeesta poiketen järjestelmää ei päivitetty ja hyppäsin tämän kohdan yli. Tämä asia on ajankohtaisempi sitten varsinaisen tuotantoympäristön Snort-koneen kohdalla. Seuraavaksi konfiguroin SSH:ta ohjeiden mukaisesti eli Root-kirjautuminen on kielletty. Eli /etc/ssh/sshd_config tiedostoon muutettiin seuraavat tiedot.

```
PermitRootLogin no
PermitEmptyPasswords no
```

Ja loin etäyhteyden kautta kirjautumista varten oman käyttäjätunnuksen ja käytän sitten su-komentoa saadakseni root-oikeudet,

```
groupadd snort
useradd -g snort snort –s /sbin/nologin
```

Seuraavaksi samalla käynnistin ssh-palvelun uudestaan, jotta muutokset tulivat voimaan.

Seuraavaksi käynnistin httpd ja mysql-palvelut, ja sitten loin hakemiston tiedostoille, jotka lataan Snortin asennusta varten. Tästä eteenpäin käytin asennuksessa windows-konetta josta olin ssh-yhdeydessä Snort-koneeseen. Oli helpompi katsoa asennuksen aikana ohjeita nettiselaimen kautta ja tutkia tarkempia tietoja seuraavaksi asennettavien ohjelmien kotisivuilta ja varmistaa uusimmat tiedostot.

Itse Snortin asennus lähti liikkeelle PCRE-kirjaston asentamisella.

```
tar –xvzf pcre-5.0.tar.gz
cd pcre-5.0
./configure
make
make install
```

Fedoran mukana oli asentunut 4.5 versio mutta asensin varmuuden vuoksi melko uuden eli 6.3 version. Sen jälkeen asensin Snortin version 2.4.3 koneelle ja loin käyttäjäryhmän ja käyttäjän Snortia varten, ja tälle tunnukselle määriteltiin no login-parametri.

```
tar -xvzf snort-2.4.3.tar.gz
cd snort-2.4.3
./configure --with-mysql
make
make install

groupadd ryhmänimi
useradd -g käyttäjänimi ryhmänimi -s /sbin/nologin
```

Sitten tein Snortin vaatimat kansiot ja kopioin tarvittavat tiedostot asennushakemistosta. Ja koska Snortin asennuspaketti ei sisällä enää Snortin sääntöjä, latasin wget-komennolla ne Snortin virallisilta kotisivuilta www.snort.org. Lisäksi halusin asentaa Bleeding Edge of Snort sivustoilta säännöt. Nämä säännöt aiheuttavat jonkin verran vääriä hälytyksiä, mutta oikein viritettynä ne näyttävät paljon hälytyksiä, joita Snortin viralliset säännöt eivät huomaa.

```
mkdir /etc/snort
mkdir /etc/snort/rules
mkdir /var/log/snort

wget http://www.snort.org/pub-
bin/downloads.cgi/Download/vrt_pr/snortrules-pr-
2.4.tar.gz
tar -xvzf snortrules-pr-2.4.tar.gz
cp -R * /etc/snort/rules
```

Seuraavaksi avattiin snort.conf-tiedosto ja sinne asetettiin perustietoja, jotta Snort saadaan käynnistettyä ja toimimaan MySQL:n kanssa. Lisäksi latasin Internet Security Gurun sivuilta snort-nimisen tiedoston, jonka sijoitin /etc/init.d hakemistoon. Tämän tiedoston avulla Snortin käynnistys ja sammuttaminen hoituu helpommin, ja snortin saa käynnistymään automaattisesti koneen käynnistyessä käyttämällä chkconfig-komentoa.

```
cd /etc/init.d
wget http://internetsecurityguru.com/snortinit/snort
```

```
chmod 755 snort
chkconfig snort on
```

Snort tukee siis kolmea eri tietokantaa MySQL:ää, MSSQL:ää ja Postgresia. Näistä valitsin käyttöön MySQL:n, koska se on valmiiksi tuttu tietohallinnon henkilöille ja sitä suositeltiin melkein joka yhteydessä missä puhuttiin tietokannoista Snortin käytössä. Ja lisäksi myös asennusohjeet suosivat MySQL:ää. Tein ohjeiden mukaan ensin ihan normaalin Snort-tietokannan, mikä sisältää tiedot hälytyksistä.

```
mysql
mysql> SET PASSWORD FOR
root@localhost=PASSWORD('password');
>Query OK, 0 rows affected (0.25 sec)
mysql> create database snort;
>Query OK, 1 row affected (0.01 sec)
mysql> grant INSERT,SELECT on root.* to käyt-
täjänimi@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql> SET PASSWORD FOR käyt-
täjänimi@localhost=PASSWORD('password_from_snort.conf')
;
>Query OK, 0 rows affected (0.25 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on
snort.* to käyttäjänimi@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on
snort.* to käyttäjänimi;
>Query OK, 0 rows affected (0.02 sec)
mysql> exit
>Bye
```

Seuraavalla komennolla tehdään snort-tietokantaan taulut.

```
mysql -u root -p < ~/snortinstall/snort-
2.4.3/schemas/create_mysql snort
```

Jotta hälytystietokanta ei paisuisi liian suureksi, tein myös samalla tavalla arkistotietokannan jonne perl kielellä tehdyn scriptin avulla siirrettäisiin vanhemmat hälytykset automaattisesti öisin. Scripti ajetaan ajastettuna joka yö.

Sitten asennetaan Base-ohjelma, jolla päästään tutkimaan nettiselaimen avulla Snortin tekemiä hälytyksiä. Base vaatii toimiakseen PHP:lle GD-kirjaston, jonka avulla PHP voi luoda lennosta kuvia. Lisäksi pitää asentaa myös ADOdb-kirjasto.

Asennus suoritettiin ohjeiden mukaan poiketen siinä, että koska käytän arkistotietokantaa, niin sen tiedot piti määritellä Base:n konfiguraatiotiedostoon.

```
cd /var/www/html
tar -xvzf base-1.2.tar.gz
rm -f base-1.2.tar.gz
mv base-1.2 base


pico base_conf.php

$BASE_urlpath = "/base";
$DBlib_path = "/var/www/adodb/ ";
$DBtype = "mysql";
$alert_dbname = "snort";
$alert_host = "localhost";
$alert_port = "";
$alert_user = "käyttäjänimi";
$alert_password = "salasana";

$archive_exists = 1; # Set this to 1 if you have an ar-
chive DB
```

Ja sen jälkeen kun Base:n toimivuus oli todettu ja laitettu toimintakuntoon, suojasin Base:n hakemiston salasanalla.

```
mkdir /var/www/passwords
/usr/bin/htpasswd -c /var/www/passwords/passwords
"base_käyttäjänimi"
```

Sitten lisättiin httpd.conf tiedostoon seuraavat rivit

```
<Directory "/var/www/html/base">
AuthType Basic
AuthName "SnortIDS"
AuthUserFile /var/www/passwords/passwords
Require user base
</Directory>
```

Tällöin kun Base avataan selaimeen, kysytään käyttäjätunnusta ja salasanaa alla olevan kuvan mukaisesti.

kuvio 4. Base:n kirjautumisikkuna

Palomuuriin tehtiin myös muutokset pääosin ohjeitten mukaan eli muun muassa ssh- ja https-protokollien yhteydet Snort-koneeseen rajoitettiin lähdeosoitteen perusteella yhteen C-luokan verkkoon. Mutta jätin vielä voimaan mahdollisuuden käyttää http-protokollaa. Mutta tulevaisuudessa käytetään vain https-protokollaa, jotta liikenne on salattua. Ja tarkoitukseen luodaan oma sertifikaatti.

```
target                 prot  opt source    destination
RH-Firewall-1-INPUT    all   --  anywhere  anywhere

Chain FORWARD (policy ACCEPT)
Target                 prot  opt source    destination
RH-Firewall-1-INPUT    all   --  anywhere  anywhere

Chain OUTPUT (policy ACCEPT)
Target                 prot  opt source    destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot   opt    source              destination
ACCEPT     all    --     anywhere            anywhere
ACCEPT     all    --     anywhere            anywhere
REJECT     icmp   --     anywhere            anywhere
icmp any reject-with icmp-port-unreachable
ACCEPT     all    --     anywhere            anywhere
state RELATED,ESTABLISHED
ACCEPT     udp    --     anywhere            anywhere
udp spt:domain
ACCEPT     tcp    --     192.168.166.0/24    anywhere
state NEW tcp dpt:ssh
ACCEPT     tcp    --     anywhere            anywhere
state NEW tcp dpt:http
```

```
ACCEPT     tcp    --     192.168.166.0/24  anywhere
state NEW tcp dpt:https
REJECT     all    --     anywhere          anywhere
reject-with icmp-host-prohibited
```

Tässä vaiheessa Snort-koneeseen asennettiin toinen verkkokortti. Kahden verkkokortin käytöstä on se hyöty, että toinen kortti hoitaa kuuntelemisen, ja toinen on koneen hallintaa varten. Koska aikaisemmin asennetulla verkkokortilla oli jo ip-osoitteet ja asetukset valmiina, niin tästä jälkiasennetusta verkkokortista oli tarkoitus tulla se kuunteleva kortti. Tälle kuuntelevalle kortille ei annettu ollenkaan ip-osoitetta, koska sen ei ole tarkoitus liikennöidä mihinkään suuntaan.

Kun Snort-prosessi käynnistettiin tällä uusimmalla kokoonpanolla niin jostain syystä Snort-prosessi vei melkein kaiken prosessoriajan. Prosenteissa tämä oli noin 70-99 koko ajan. Aiemmin kun Snort-prosessia ajettiin yhdellä verkkokortilla kokeen vuoksi, niin prosessorin käyttöaste ei Snortin käytössä noussut juuri ollenkaan 20 prosentin yli. Pääasiassa luku pysytteli alle 10%. Ja kun asetusten vaihtaminen suoraan ifcfg-eth0 ja ifcfg-eth1 tiedostoihin päikseen ei onnistunut, ei ratkaisuksi tullut muuta kuin irroittaa verkkokortit kokonaan koneesta, antaa Linuxin poistaa vanhat asetukset ja asentaa ne varmuuden vuoksi yksitellen uudestaan. Asennuksen jälkeen Snortin käytössä oli nyt eri verkkokortti kuunteluun, ja tämän kortin kanssa Snort-prosessi ei nostanut prosessorin käyttöastetta enää liian korkeisiin lukemiin, vaan lukemat olivat pääasiassa 0-20 välillä. Se, miksi toinen verkkokortti kulutti melkein kaiken prosessoritehon, ei selvinnyt varsinkin kun verkkokortit olivat tyypiltään täysin identtiset ja verkon liikennettä tutkittiin samasta paikasta molemmilla kerroilla. Ja kummallakaan kerralla ei kumpikaan verkkokortti tcpdump:lla tehdyn tutkimuksen mukaan pudottanut yhtään pakettia, joten verkkoliikenteessäkään ei ole tapahtunut mitään ihmeellistä. Jostain syystä verkkokortti ei tullut toimeen Snortin kanssa.

Nyt ensimmäiseksi Snort laitettiin tutkimaan liikennettä Päijät-Hämeen koulutuskonsernin verkon palomuurin ulkopuolelle. Tässä käsitellään ensin, millaisia hälytyksiä Snort teki ollessaan palomuurin ulkopuolella ja sen jälkeen keskitytään hälytyksiin, jotka tulivat Snortin ollessa sille alun perin tarkoitetussa paikassa eli DMZ:ssa. Loogisessa kuvassa, joka on liitteenä 1, PHKK:n DMZ-alue näkyy laitimmaisena oikealla.

9.2 Snort palomuurin ulkopuolella

Snortin säätäminen aloitettiin lyhyen hälytyksien seurailun jälkeen rajoittamalla paria hälytystä. Molemmat liittyivät MS-SQL-tietokantasovellukseen ja tarkemmin sanoen Slammer-matoon, joka yrittää aiheuttaa puskurin ylivuodon ja saastuttaa koneen. Tämä ongelma ilmenee vain päivittämättömissä koneissa. Itse päivitys oli julkaistu jo 2002 heinäkuussa kun taas Slammer iski vasta 25. tammikuuta 2003. Slammerin aiheuttamat hälytykset olisivat kasvattaneet nopeasti Snortin hälytystietokannan hyvin suureksi, ja se olisi hidastanut huomattavasti tietokannan käyttöä ja näin ollen haitannut muiden hälytysten tutkimista. Slammer ehti aiheuttaa 3200 hälytystä 50 minuutissa, joten tämän tutkimuksen kannalta toimenpide oli tarpeellinen.

Täytynee myös harkita NMAP ping-hälytyksen poistamista käytöstä, koska Snort tekee hälytyksen jokaisesta ping-paketista jonka kuorman koko on nolla. Snortin kotisivut myös mainitsee kyseisen säännön heikkoudet ja myöntää sen, että se aiheuttaa vääriä hälytyksiä. Vaikka Snort aihuttaa jonkin verran vääriä hälytyksiä, niin myös ihan aiheellisia hälytyksiä tulee. p2p-ohjelmista BitTorrent aiheutti jonkin verran hälytyksiä, mutta huomattavasti vähemmän kuin ns. testiverkossa eDonkey aiheutti. Johtunee varmaankin ohjelmien eroavaisuuksista ja siitä että konsernin palomuuri pystyy estämään osan p2p-ohjelmien liikenteestä. Testiverkossa tähän ei ollut mahdollista puuttua.

Aika monta hälytystä tuli myös SSH-scannauksesta, jossa yksi lähdeosoite pommitti läpi 653 kohdeosoitetta konsernin verkosta. Muita toimenpiteitä ei

kyseisestä lähdeosoitteesta tehty verkkoa kohti. Se mikä scannauksen tarkoitus oli, jäi epäselväksi. Voi olla, että tarkoituksena oli saada tietoa salasanoista tai käytettävästä autentikoinnista. Lähdeosoitteen perusteella scannaus tuli Dallasista Yhdysvalloista.

Sama kohdeverkko kiinnosti myös päivää myöhemmin kun oman verkon ulkopuolelta yksi lähde lähetti 1916 ping-pakettia 1840 eri kohdeosoitteeseen. Lähdeosoite sijaitsi Kiinassa. Kohteet olivat hyvin pitkälti samoja kuin ssh-scannauksessa. Tässä tapauksessa syynä voi olla mahdollisesti myös Nachi / Blaster-madon saastuttama kone.

Snort huomasi myös muita erilaisia viruksia ja matoja. MyDoom.F-mato aiheutti muutaman hälytyksen, koska ainakin pari kohtaa sähköposteissa sopi kuvaukseen, erikoinen otsikko ja liitteen nimi ja tiedoston tunniste. Samanlaisia hälytyksiä aiheuttivat SVEN.A mato, Netsky.p mato ja MyDoom.I mato.

Snort tunnisti paljon erilaisia haitta- ja vakoiluohjelmia, ja nämä hälytykset näkyivät Bleeding snort-sääntöjen ansiosta. Ja nopean tutkailun jälkeen nämä hälytykset pitivät jokseenkin paikkaansa. Tietysti verkossa liikkuessa myös vahinkoja sattuu ja näihin ohjelmiin törmää helposti.

Erilaiset web-palvelut ovat myös useiden hyökkäysyritysten kohteina monien haavoittuvuuksien takia. Yksi eniten hälytyksiä aiheuttanut hyökkäys oli kohdistettu PHP-sovellusten XML-RPC-kirjastoa vastaan. Hälytyksiä aiheutuu myös aikuisviihdesivuilla käynnistä ja kuten normaali verkossa surffailija tietääkin näitä kyseisiä sivuja ja mainoksia ilmestyy eteen ilman omaa vaikuttamista asiaan.

9.3 Snort DMZ-alueella

Snort jätettiin tutkimaan verkkoa yön yli, jonka jälkeen aamulla tehtiin ensimmäiset säädöt. Meluisin sääntö koski proxy-kyselyitä, jotka tapahtuivat verkon sisällä. Toinen sääntö, jonka ilmoittelua piti säätää, koski perl-scriptiä nimeltään

calendar_admin.pl. Tosiasiassa liikenne liittyi moodle-palveluun ja siellä sijaitsevaan kalenteriin. Joten kyseessä oli lukuisat väärät hälytykset. Samoin paljon hälytyksiä tuli avoimien porttien tiedustelusta, joka johtui siitä, kun ameba.lpt.fi otti yhteyttä irc.cc.tut.fi palvelimeen. Kyseessä on kuitenkin normaali liikenne, joten nämä hälytykset oli hyvä jättää huomioimatta niiden meluisuuden takia.

Ja kokeeksi otimme takaisin käyttöön säännön, joka hälytti Slammer-madosta. Palomuuri esti nämä hyökkäykset kokonaan, ja DMZ-alueella ei näitä paketteja enää liikkunut. Myös SSH-scannauksista tuli hälytyksiä, ja lähdeosoitteita oli neljä kappaletta. Kolme näistä tuli ulkomailta: Yhdysvalloista, Belgiasta ja Espanjasta, ja yksi Suomesta. SSH-pakettien tulee olla kuitenkin sallittuna palomuurissa, jotta normaali SSH-liikenne ei tule estetyksi. Tämän asian vuoksi myös ei toivottu SSH-liikenne pääsee liikkumaan vapaasti. Myös laajamittaisemmat pingaukset jatkuivat täällä DMZ-alueella. Tällä kertaa yhdestä lähteestä tuli 4789 pakettia 4659 kohdeosoitteeseen. Pingit tulivat tällä kertaa myös Kiinasta ja samasta verkosta mutta eri osoitteesta.

DMZ:n puolelta Snort teki hälytyksiä seuraavista viruksista: Zafi, MyDoom.I, NetSky.P, MyDoom.F, Swen.A, KillBill, MyDoom/MIMAIL.R, Evaman. Pystyin sen verran tutkimaan paketteja, jotka aiheuttivat näitä hälytyksiä, että monet näistä liittyivät sähköposteihin ja niiden mukana kulkeneisiin liitteisiin. Esimerkkinä viesti, joka alkaa greetings from france, your friend ja liitteenä on tiedosto letter.zip. Ja Zafi-virus yrittää houkutella käyttäjää avaamaan sähköpostiviestin, jonka otsikkona on eE-postikorti!. Harmillinen kirjoitusvirhe on päässyt mukaan otsikkoon, mutta helpottaa huomattavasti virusten havaitsemista, kun viesti ei sekoitu oikeiden viestien kanssa.

Tutkiessa joukkoa loopback traffic-hälytyksiä, törmättiin tapahtumaan, jossa jostain syystä ameboid.lpt.fi palvelin yrittää liikennöidä osoitteeseen 127.0.0.2. Tämä tapahtuma lähti liikkeelle siitä, että orbs.dorkslayers.com otti yhteyttä ja ameboid luotti nimipalvelimeen, joka antoi osoitteeksi 127.0.0.2. Tämä ongelma voidaan korjata lisäämällä muutama rivi named.conf-tiedostoon, jolloin kyseistä liikennettä ei ameboid.lpt.fi puolesta tapahdu.

Myös BASE tarvitsi hieman lisää säätämistä. Edellisessä asennuksessa oli jäänyt asentamatta pear image graph, jolla ohjelmaan saadaan lisää graafisia ominaisuuksia kaavioiden muodossa. Ohjelmaa asennettaessa se ilmoitti vaativansa image_canvas-pakettia, joka taas asennettaessa vaati image_color-pakettia. Näiden kahden paketin asennuksen jälkeen myös pear image graph suostui asentumaan. Jotta Snortin tietokannat pysyisivät siistissä muodossa, otettiin käyttöön archiveplus ja purge_database-ohjelmat. Työtä viimeistellessä tuli eteen tieto, jonka mukaan tunkeutumisen havaitsemisjärjestelmä on hyvä keino havaita DHCP-huijaukset. Hyökkäykseen tarvitaan vale DHCP -palvelin ja hyökkäys tapahtuu siten, että väärennetään DHCP release-viestit oikeilta asiakkailta ja sitten varataan osoitteet omaan käyttöön, lisäksi odotetaan, että oikeiden asiakkaidet leaset päättyvät. Ja kun oikealta DHCP-palvelimelta ovat IP-osoitteet loppuneet, niin vale-palvelin alkaa jakamaan IP-osoitteita ja verkkoparametreja, joissa voi olla väärennettynä oletusreititin ja DNS-palvelin.

Esimerkki Snortin DHCP-säännön luomiseen löytyy Robert Currien artikkelista, joka löytyy osoitteesta http://security.itworld.com/4363/ITW3542/pfindex.html. Itse sääntöä kuitenkin muutettiin sen verran, että pass-kohdat jätettiin kokonaan pois. Tällä saatiin se etu, että Snortia ei tarvitse käynnistää –o parametrilla, joka aiheuttaa hälytysjärjestyksen muutoksen eli pass-säännöt käsitellään ennen alert-sääntöjä. Nyt ei ole vaaraa, että huonosti kirjoitettu pass-sääntö kumoaisi alert-sääntöjä. Eli sääntö oli muotoa:

```
alert udp ![192.168.xxx.xxx,193.166.xxx.xxx] 67 -> any
68 (msg: "Rogue DHCP server"; sid:1000002; priority:1;
classtype:misc-attack;)
```

Hälytys siis tapahtuu kun lähetetään portista 67 DHCP-vastaus muusta kuin oikeasta DHCP-palvelimesta, mihin tahansa kohdeosoitteeseen ja porttiin 68. Lisäksi hälytykselle asetettiin korkein prioriteetti.

9.4 Bro IDS:n asennus ja testaus

9.4.1 Bro IDS:n vaatimuksia

Bro asennettiin tavalliseen työasemakoneeseen, jossa oli prosessorina AMD Athlon 1800+, 256 MB keskusmuistia, 36 GB IDE kiintolevy ja kaksi 10/100Mbps verkkokorttia. Brohon suositellaan 1GHz:n prosessoria, kun liikenne on keskimäärin alle 5000 pakettia sekunnissa Ethernet 100Mbps-verkossa. Kun siirrytään Gigabitin Ethernet-verkkoon ja liikenne on vielä alle 10000 pakettia sekunnista, täytyisi käytössä olla 2 Ghz:n prosessori. Ja kun liikenteen määrä saavuttaa 50000 paketin sekuntinopeuden olisi käytössä hyvä olla 4 GHz:n prosessori. Nämä vaatimukset eivät ole mitään absoluuttisia vaan suuntaa antavia, ja niihin vaikuttaa myös liikenteen sisältö.

Bro toimii Unix-järjestelmissä mukaan lukien Linux ja Solaris, mutta tekijät suosittelevat FreeBSD:tä. Itse asensin Bro:n koneeseen jossa oli Fedora Core 3 käyttöjärjestelmä, eikä suurempia ongelmia ole tullut itse käytössä tai suorituskyvyssä liittyen itse käyttöjärjestelmään. Keskusmuistia Bro:n käyttöön suositellaan vähintään 512 Mb, jos käytössä on pieni verkko: noin 200 laitetta 100Mbps:n yhteydellä. Jos kyseessä on isompi verkko, niin 1 GB on vaatimus ja suositellaan 2-3 GB keskusmuistia. Koska IDS-järjestelmä tuottaa paljon tietoa lokeihin ja tietokantoihin, jos sellainen on käytössä, niin myös kiintolevyn oikea koko on tärkeää. Vähimmäissuositus on 10 GB, ja suosituksena 50 GB

Tässä niin sanotussa testiverkossa, mihin asensimme Bro:n, on noin 250 laitetta joten liikuimme laitteistosuositusten rajoilla suorituskyvyn osalta. Prosessorin käyttöaste jäi kohtalaisen alhaiseksi, mutta koko keskusmuisti oli eri prosessien käytössä. Mitään hidastumisia ei käytönaikana silmämääräisesti näkynyt ja uskoisin, että Bro on ehtinyt kaikki paketit tarkistaa. Tätä ei pysty mitenkään varmistamaan, koska en löytänyt vastaavanlaista toimintoa, kuten Snortin performance monitor.

9.4.2 Bro IDS:n asennus

Käyttöjärjestelmäksi valitsin siis Fedora Core 3:n joka oli minulle jo tuttu käyttöjärjestelmä, kun testailin Snortia. Tarkoituksena oli siis valita tuttu ja turvallinen alusta, jotta kaikki menisi sulavasti asennuksen ja testauksen aikana. Koska suorituskyky oli tärkeää, pyrin tekemän Fedora Core 3:n asennuksesta mahdollisimman kevyen ilman mitään turhia komponentteja. Mukaan otettiin lähinnä verkonhallintaan ja käyttöön vaadittavia osia, www-serveri, järjestelmän hallintatyökalut ja tarvittavat tekstieditorit. Tähän asennukseen otin mukaan kokeeksi myös graafisen Linuxin ja tarkemmin sanottuna KDE-työpöytäympäristön, josta oli hyötyä lähinnä asennuksen alkuvaiheessa, asennusohjeita ja manuaaleja tutkiessa.

Bro:sta asennettiin versio 0.9a10, joka oli lataushetkellä uusin versio. Itse asennus meni ihan normaalisti ilman ongelmia. Toimiakseen Bro vaatii asennettavaksi Perlin version 5.6 tai uudemman, libpcap:in version 0.7.2 tai uudemman ja vielä lisäksi tcpdump:in version 3.8 tai uudemman.

9.4.3 Bro IDS:n konfigurointi

Konfigurointi voidaan tehdä käsin tai bro_config-scriptin avulla. Itse käytin bro_config-scriptiä, joka toimi pääosin oikein. Konfiguroinnissa määritettiin, mikä on Bro:n arkistointihakemisto, millä käyttäjänimellä Bro:ta ajetaan ja mitä verkkoliitäntää Bro kuuntelee.

Sitten määriteltiin päivittäisten raporttien muoto. Ensin raportin nimi, sitten mistä kellonajasta lähtien raportti luodaan ja kuinka monen tunnin ajalta, sitten voidaan määritellä, jos halutaan lähettää raportti tiettyihin sähköpostiosoitteisiin ja halutaanko sähköpostiviestit salata.

Seuraavaksi piti Bro:n tutkia itsestään verkon konfiguraatiota, jotta se olisi voinut määrittää tutkittavan verkon mutta ainakaan itse en saanut sitä toimimaan, joten

määritin käsin local.site.bro-tiedostoon paikalliset lähiverkot. Huomasin myös jonkin ajan kuluttua, että Bro ei oletuksena tunnistanut VLAN-tageja. Manuaali ei tähän osannut neuvoa ratkaisua, mutta onneksi Internetin hakupalveluiden kautta löytyi ratkaisu tähänkin. Oletuksena eivät olleet Bro:ssa käytössä myöskään hyökkäysten tunnistamiseen tarvittavat säännöt. Ne aktivoitiin samassa tiedostossa kuin VLAN-tagien tunnistaminen eli local.site.bro-tiedostossa, joka löytyy osoitteesta $BROHOME/site/. VLAN-tuki otetaan käyttöön kirjoittamalla rivi @load vlan.

Seuraavaksi muutettiin sig-action.bro-tiedostoa, joka sijaitsee Bro:n policy-hakemistossa. Tiedostossa määritellään, kuinka reagoidaan, kun Bro havaitsee liikenteessä yhteneväisyyksiä sen sääntötiedostoihin. Voidaan olla joko kirjaamatta ollenkaan tietoa havaitsemisesta, kirjataan normaalisti hälytystiedostoon, sitten kirjataan kerran per kyseinen lähde tai kirjataan hälytys vain kertaalleen eikä sen jälkeen kyseisiä hälytyksiä noteerata.

9.4.4 Bro IDS:n käyttö

Bro käynnistetään taustaprosessiksi komennolla bro.rc start. Tämän jälkeen Bro alkaa kirjaamaan tapahtumia eri tiedostoihin logs-hakemistoon. Yksi iso Bro:n puute tulee tässä esiin, nimittäin siltä puuttuu graafinen käyttöliittymä, jossa voisi selata melkein reaaliajassa hälytystietoja muussakin muodossa kuin tämänhetkisessä tekstitiedostoformaatissa. Aikaisemmin mainitut Bro:n raportit ovat ihan käyttökelpoisia tutkittaessa tapahtumia pidemmältä aikaväliltä, kuten useamman tunnin tai yhden vuorokauden ajalta. Bro:hon on todennäköisesti tulossa jossain vaiheessa graafinen käyttöliittymä, mutta siitä ei ole tällä hetkellä olemassa edes testiversiota jaossa.

Raportti sisältää kyllä ihan kiinnostavia tietoja yksittäisistä hälytyksistä muun muassa, milloin yhteys on muodostettu, kuinka kauan yhteys kesti ja mitä portteja käytettiin. Lisäksi raportista näkee verkossa tehdyt scannaukset lähde ja kohdeip-osoitteineen. Raportista löytyy myös Top 20-listat eniten liikennöivistä ip-

osoitteista ja niistä ip-osoitteista, joihin on eniten liikennettä. Eniten käytetyt palvelut oli myös listattu, joukosta löytyi esim. DNS, Netbios-ssn ja http. Viimeisenä oli listattu eniten liikennöineet ip-osoiteparit. Itse kaipaisin tähän tekstimuotoiseen raporttiin vielä tietoja yleensä liikenteen määristä, eli kuinka paljon paketteja on tutkittu. Ja jos Bro on joutunut pudottamaan paketteja pois ruuhkan takia, niin nekin olisi hyvä listata.

Kun Bro oli saatu käyntiin, kiinnittyi huomio siihen, että Bro:n sääntöjä ei tällä hetkellä ole vielä mahdollista päivittää. Eli säännöt päivittyvät tällä hetkellä mahdollisesti vain uuden Bro:n version ilmestyessä. Tulevaisuudessa päivitystä varten on tulossa scripti, joka käyttää wget-komentoa tiedoston lataamiseen, jonka jälkeen scripti huolehtii säännöt oikeisiin tiedostoihin. Sen jälkeen Bro käynnistyy uudestaan uusien sääntöjen kanssa.

9.4.5 Snortin ja Bro IDS:n tulosten vertailua

Snort ja Bro laitettiin molemmat tässä testivaiheessa tutkimaan varsin pientä PHKK:n verkon osaa eli yhden rakennuksen liikennettä, eli talon sisäistä, sieltä lähtevää ja sinne saapuvaa liikennettä. Ja vielä tarkemmin sanottuna tietoturva-aluetta nimeltään PHKK-henkilökunta, joka näkyy liitteessä 1. Ensinnäkin tulosten määrässä oli valtava ero, eli Snort antoi huomattavasti enemmän hälytyksiä kuin Bro, mikä johtuu useista eri asioista. Ensinnäkin vaikka sainkin Bro:n toimimaan, en ole täysin varma, toimiko se vielä täydellä teholla. Tässä kohtaa tulee esiin open source-ohjelmien huono puoli eli kunnon asennusohjeita tai manuaaleja ei ole olemassa. Tietysti ohjelmien kotisivuilta löytyy jonkinlaiset ohjeet, mutta nekin jättivät joitakin asioita epäselviksi. Snortin eduksi on laskettava sen hyvin päivittyvät säännöt verrattuna Bro:n vastaaviin joita ei vielä ole mahdollista päivittää mistään.

Molemmat ohjelmat kuuntelivat samaa verkkoa samaan aikaan yhden vuorokauden ajan. Snort teki tässä ajassa 443271 hälytystä, joista on nähtävänä liitteessä 2 pieni Snort Report-ohjelman näkymä, kun taas Bro teki 9723 hälytystä. Bro:n raportista,

josta on näyte liitteenä numero 4, käy ilmi myös että varsinaisia kiinnostavia tapahtumia oli 147, joista onnistuneita oli 101 ja epäonnistuneita 46. Tapahtuma muodostetaan, jos yksi tai useampi hälytys aiheutuu kun liikennettä tunnistetaan. Verkon skannauksia Bro havaitsi 11, jotka se määritteli kaikki onnistuneiksi. Nämäkin skannaukset tulivat verkon sisäisistä osoitteista ja kohdistuivat verkon sisälle. Ja ip-osoitteista pystyin päättelemään että liikenne oli sallittua tutkailua.

Sen verran ohjelmien sääntötiedoissa on eroa, että se liikenne, minkä Snort tunnistaa turvattomaksi SNMP-liikenteeksi, niin Bro tunnistaa sen hyökkäykseksi, joka on kohdistettu UDP-porttiin 161 ja jonka tarkoituksena olisi kaataa Bay/Nortel Nautica Marlin silta. Tässä huomataan hyvin, kuinka erehtyväisiä Snortin ja Bro:n säännöt ovat. Tässäkin oli kyseessä täysin tavallinen SNMP-liikenne.

TFTP-tulostuspyynnön molemmat ohjelmat havaitsivat samalla lailla. Tämä hälytys voidaan luokitella vääräksi hälytykseksi, josta Snortinkin sääntöjen kuvauksissa on maininta. Hälytyksen laukaisi kytkimen lähettämä paketti.

Bro kirjasi hälytyksiin myös yhden troijalaisen nimeltään BACKDOOR DeepThroat 3.1. Snortista kyseinen hälytys löytyy myös, mutta nykyään se on poistettu käytöstä syystä, joka ei minulle selvinnyt. Bro:n tiedoista kävi ilmi, että tämä yritys olisi todennäköisesti epäonnistunut. Seuraava merkintä Bro:n raportissa oli merkitty yritykseksi päästä www-palvelimelle. Kyseessä oli kuitenkin vain virhetilanne http-liikenteessä, jota Snort ei ollut ollenkaan huomioinut. Bro ilmoitti myös, että olisi tapahtunut hyökkäyksen yritys IDS-järjestelmää kohtaan. Lähdeosoite oli kuitenkin verkon sisältä ja sellaisesta koneesta, josta tuskin lähtee kyseistä liikennettä ulospäin. Snort oli huomioinut liikenteen, mutta oli antanut sille alimman prioriteetin eikä nähnyt sitä varsinaisena hyökkäyksenä.

Tässä oli lyhyesti käsiteltynä ne tapahtumat, mitkä Bro havaitsi. Snortilta löytyi huomattavasti enemmän tapahtumia ja näiden tapahtumien tutkiminenkin on paljon helpompaa hyvien apuohjelmien kanssa. Käyn tässä läpi vain korkeimman prioriteetin ja muuten vaan kiinnostavat hälytykset, koska jo ykkösprioriteetin

hälytystyyppejä oli 25 erilaista, vaikkakin monet hälytystyypit liittyvät usein samaan tapahtumaan.

Eniten hälytyksiä aiheutti P2P-ohjelma eDonkey, jonka käyttö laukaisi hälytyksiä tiedostokyselyistä, yhteyden muodostuksista servereille ja vastauksista tiedostokyselyihin. Lisäksi sama lähdeosoite aiheutti hälytyksiä myös toisen p2p-ohjelman käytöstä, joka oli Gnutella. Tiedot Snortin kaappaamista paketeista kertoivat selkeästi, että hälytys oli oikea molempien ohjelmien kohdalla.

Koska tässä Bro:n ja Snortin testissä ei konfigurointia tehty paljon, niin myös vääriä hälytyksiä aiheutui jonkin verran. Yksi väärä hälytys aiheutui normaalista Windows server 2003:n ja toisen Windows-koneen välisestä liikenteestä. Tämän Snort tulkitsi hyökkäykseksi, jotka on tarkoitettu ISS:n Realsecure ja BlackIce tuotteita vastaan.

Hälytyksiä aiheutti monessa paikassa myös MSN messenger-ohjelman käyttö. MSN messengerissä on ollut paljon tietoturva-aukkoja ja niitä on todennäköisesti monia vielä jäljellä. Microsoft onkin kehoittanut poistamaan ohjelman yrityskoneista. Lisäksi yksi kone näyttäisi sisältävän liikenteen perusteella ainakin kahdenlaisia haittaohjelmia, jotka lähettävät tietoja eteenpäin verkkoon. Liikennöinti ei jatkunut kovin säännöllisenä, joten haittaohjelmat eivät ole kovin aktiivisia tai ne on poistettu koneelta.

Myös hotmail aiheutti jonkin verran hälytyksiä. Snort kirjasi hälytykset, postilaatikkoon kirjautumisessa ja sähköpostiviestin lähettämisestä sekä lukemisesta. Hotmail on varmasti päässyt mukaan Snortin sääntöjen joukkoon johtuen monista tietoturvaongelmistaan. Samasta syystä myös Skype on mukana säännöissä, ja pari Skypeen liittyvää hälytystä tuli Snortilta.

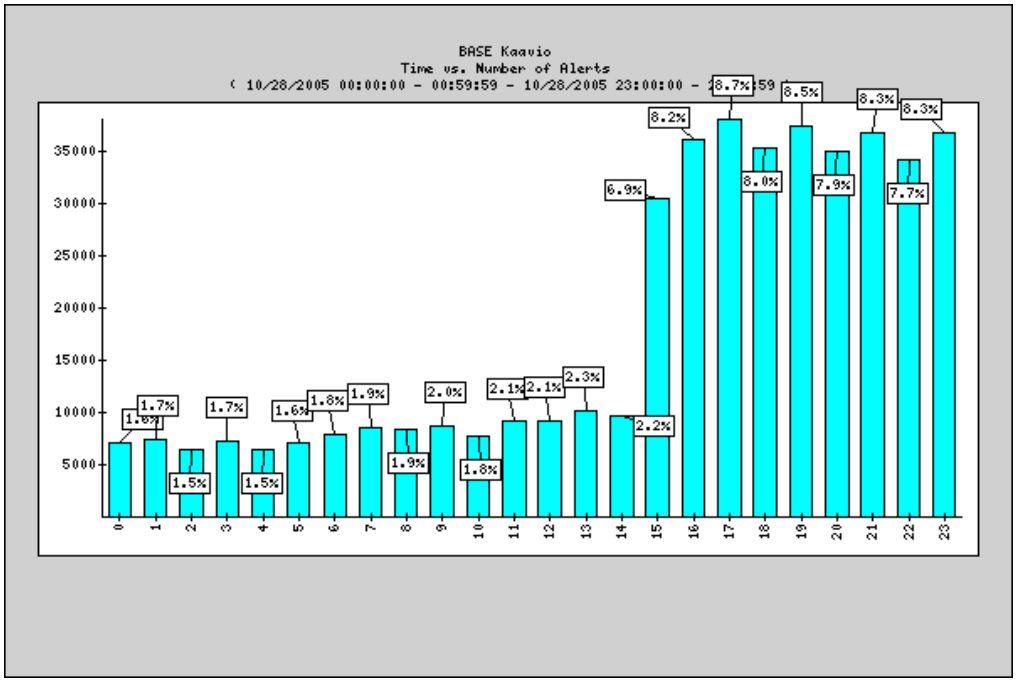
Kun verrataan, kuinka hälytykset eroavat Snortin tekemän alert-tekstitiedoston ja Base:n luoman html-tiedoston välillä, niin ensimmäisenä huomaa todennäköisesti ulkoiset seikat. Liite 5 esittää, kuinka Base-ohjelma näyttää Snortin hälytyksen, ja alla on sama hälytys tekstimuodossa alert-tekstitiedostosta.

[**] [1:2001219:12] BLEEDING-EDGE Potential SSH Scan [**]
[Classification: An attempted login using a suspicious username was detected] [Priority: 2]
03/28-04:00:27.041705 59.106.12.187:35654 -> 193.166.xxx.xxx:22
TCP TTL:47 TOS:0x0 ID:56739 IpLen:20 DgmLen:60 DF
******S* Seq: 0x85E06287 Ack: 0xF9A55D7E Win: 0x16D0 TcpLen: 40
TCP Options (5) => MSS: 1380 SackOK TS: 360038180 0 NOP WS: 0

[Xref => http://www.whitedust.net/article/27/Recent%20SSH%20Brute-Force%20Attacks/]

Molemmissa tapauksissa näkyvät alussa järjestysnumerot, jotka eivät täsmää, koska Base:n järjestysnumero on nollaantunut tietokannan uudelleenluonnissa. Molemmissa näkyy tieto siitä, mikä hälytys on kyseessä. Base ei näytä tässä näkymässä tekstitiedostossa näkyvää luokittelu- tai prioriteetti-tietoa, jotka kuitenkin ovat talletettuna tietokantaan ja näkyvät toisella yleisemmällä sivulla. Seuraavaksi esitetään hälytyksen ajankohta ja lähde- ja kohde ip-osoitteet ja portit. Base näyttää sitten hiukan tarkemmin paketin tietoja kuin Snortin alert-tiedosto johtuen varmaankin ihan tilankäyttösyistä.

Kuviossa 5 on esitetty, kuinka Snortin hälytykset ovat jakautuneet kellon ajan mukaan ja kuvio on muodostettu BASE:n avulla. Suuria johtopäätöksiä pelkästään tästä kuvasta ei voi vetää, koska tarkempaan analysointiin tarvittaisiin huomattavasti enemmän materiaalia. Hälytysten määrä alkoi kasvamaan, kun kello oli yli kolme iltapäivällä. Yhden johtopäätöksen kellon ajasta voi vetää, että Atlantin toisella puolella on aamu ja ihmiset ovat aktivoituneet siellä päin maailmaa. Mitään uutta haavoittuvuutta ei ollut ilmestynyt lähipäivinä, joka olisi voinut selittää tapahtuneen. On myös mahdollista, että kyseessä voi olla jonkinlainen verkon yli tapahtuva varmuuskopiointi.



Kuvio 5. Snortin hälytykset 20.10.2005

10. YHTEENVETO

Arvioitaessa työn onnistumista voidaan todeta, että vaikka tähän työhön ei saatu mukaan tarkkoja tietoja, kuinka tuontantoympäristöön tarkoitettu laite suoriutuu testikonetta paremmin, niin saatiin kuitenkin selville kaikki tarvittavat tiedot siitä, kuinka asennus tulee suorittaa ja mitä muita toimenpiteitä ja ohjelmia laitteen toimintakuntoon saattamiseen tarvitaan. Vaikka itselläni ei linux-käyttöjärjestelmistä ollutkaan paljoa kokemusta, niin kynnys ryhtyä käyttämään linuxia oli yllättävän matala. Omien kokemusten pohjalta voin suositella lämpimästi linuxia vastaavanlaisissa tapauksissa.

Tunkeutumisen havaitsemisjärjestelmän käyttöönoton tavoitteena oli saada tietoa, kuinka konsernin palomuurit toimivat, jotta voidaan luoda asiasta raportteja asiasta kiinnostuneille tahoille. Myös DMZ-alueella olevaa epämääräistä liikennettä oli tarkoitus saada analysoitua ja tunnistettua, jotta tiedetään mihin varautua. Koska tarkoitus oli asentaa vain yksi sensori, täytyi miettiä tarkkaan, mikä on se paikka jota tulisi valvoa eli onko se esimerkiksi työasema vai palvelin VLAN:it. Koska DMZ-alueella sijaitsee tärkeitä palvelimia, joiden tulisi olla käytettävissä koko ajan, on järkevää kohdistaa havainnointi tälle alueelle, jotta tiedetään minkälaisia mahdollisia hyökkäyksiä näihin koneisiin kohdistuu.

Ja näitä tietoja saatiinkin alkuun vähän liikaakin ennen kuin Snort-ohjelmisto oli saatu hienosäädettyä eli saatu eroteltua, mikä on normaalia liikennettä ja mikä vihamielistä liikennettä. Eli alussa tulee paljon vääriä hälytyksiä ja se vaatii jonkin verran työtä että nämä saadaan selvitettyä. Kun nämä alkutoimet on saatu suoritettua, on käsissä työkalu, josta saatuja tietoja voidaan käyttää analysointiin ja raportointiin. Hyökkäystietojen lisäksi Snortilla voi mahdollisesti paljastua eri ohjelmien väärin asetetut konfiguraatiot, jotka näkyisivät virhetilanteina verkkoliikenteessä.

Snort-ohjelmisto oli jo alun perin vahvoilla valittavaksi ohjelmistoksi, ja koska varteenotettavaa kilpailijaa ei open source piireissä ollut, niin valinta oli selkeä. Snortin tiedetään pystyvän analysoimaan hyvinkin suuria liikennemääriä, mikä oli

myös kanssa vaikuttava kriteeri valittaessa tunkeutumisen havaitsemisjärjestelmää Päijät-Hämeen koulutuskonsernin verkkoon, jossa on paljon liikennettä. Jos valinnassa olisi jouduttu turvautumaan kaupalliseen järjestelmään, olisivat kulut olleet huomattavasti suuremmat. Gigabitin nopeuteen pystyvät laitteet maksavat kymmeniä tuhansia euroja ja päälle tulevat vielä ylläpitokustannukset.

Asennusvaiheessa oli huomattavasti apua tekstissäkin mainitusta internetsecurityguru.com sivustoilta löytyneestä ohjeesta. Asennusohjeet lähtivät liikkeelle käyttöjärjestelmän asennusvaiheesta, jossa jo neuvottiin tarkoin mitä paketteja kannattaa valita, jotta järjestelmä olisi mahdollisimman kevyt, mutta sisältäisi kaikki tarvittavat komponentit.

Snortin hälytysten tutkiminen on hyvinkin helppoa varsinkin Base:n avulla. Laajojen hakuvaihtoehtojen kanssa pystyy löytämään tietokannasta juuri ne tiedot, mitä tarvitaan. Hakuparametreinä voidaan käyttää muun muassa päivämääriä, kellonaikoja, ip-osoitteita ja sanahakua. Näillä pystytään keräämään tarkka otos tiedoista vaikka raportointia varten.

Kun nyt myöhemmin on saatu asennettua tuotantokäyttöön tarkoitettu palvelinkone, niin suurin ero näkyi itse Snortin suorituskyvyssä ja tarkemmin sanottuna kyvyssä saada tutkittua mahdollisimman suuri osa verkossa liikkuvista paketeista. Kun testikokoonpanolla Snort saattoi pudottaa normaalisti noin 5-10% paketeista, niin tällä uudella palvelimella pudotettujen pakettien osuus putosi jopa 0,009% paketeista. Sillä hetkellä, kun Snort käynnistetään, niin paketteja hukkuu jonkin verran, mutta se asia täytyy hyväksyä, ja paketteja jää myös silloin havaitsematta kun Snort täytyy käynnistää uudestaan esimerkiksi uusien sääntöjen käyttöönotossa. Valitettavasti samanlaista suorituskykyeroa uuden kokoonpanon hyväksi ei havaittu MySQL-tietokantaa käyttäessä, vaikka käyttäminen onkin sujuvampaa koska koneen resursseja on enemmän vapaana. Lisäksi kun käytössä on moniydinprosessori, niin kuormaa voidaan jakaa.

Jotta kilpajuoksussa hyökkääjiä vastaan pysytään mukana, on elintärkeää pitää itse Snort ja säännöt ajan tasalla. Nopea reagointi on avainasemassa siinä, että

mahdolliset vahingot pysyvät mahdollisimman pieninä. Snortia käytettäessä on vain muistettava, että Snort ei itsessään estä mitään vahingollista liikennettä vaan kertoo, jos tämänlaista liikennettä on verkossa. Joten valvontavastuu jää hyvin pitkälti ihmisen harteille ja säännöllinen hälytysten seuraaminen on tärkeää, jos on epävarma oman verkon tietoturvasta. Täytyy myös muistaa, että hyökkääjät ovat aina askeleen edellä. Tietoturva on aina monen asian summa ja kaikkeen on syytä varautua. Tunkeutumisen havaitsemisjärjestelmät ovat tulleet jäädäkseen yhdeksi työkaluksi virustorjuntaohjelmien ja palomuurien rinnalle.

LÄHTEET

Andrés, S., Kenyon, B. 2004. Security Sage's Guide to Hardening the Network Infrastructure. Syngress Publishing, Rockland, MA, USA.

Beale, J., Caswell B., Foster, J. & Posluns J. 2003. Snort 2.0 Intrusion Detection. Syngress Publishing, Rockland, MA, USA.

Beale, J., Caswell, B. 2004. Snort 2.1 Intrusion Detection , Second Edition. Syngress Publishing, Rockland, MA, USA.

Northcutt, S., Novak, J. 2001. Verkkomurtojen havaitseminen. Talentum Media Oy, Helsinki.

About Snort. 2005. http://www.snort.org/about_snort, 17.10.2005

Basic Analysis and Security Engine (BASE) project, 2004. http://secureideas.sourceforge.net, 2.3.2006

Bro intrusion detection system, 2005. http://www.bro-ids.org, 17.10.2005

Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Service Module, 2006. http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00801e55dd.html, 7.4.2006

Cisco IPS 4200 Series Sensors, 2006. http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/index.html, 7.4.2006

Dragon 7 network intrusion detection and prevention, 2006 http://enterasys.com/products/ids/DSNSS7/DSNSS7.pdf, 7.4.2006

Internet security – iss datenblaetter, 2005.

http://www.internet-security.ag/gen/iss/e0000000000.php, 18.10.2005

Intrusion SecureNet Sensor, 2003.
http://www.intrusion.com/products/documentation/brochures/securenet_sensor.pdf
, 10.10.2005

Mitä on tunkeutumisenhavaitseminen?, 2005.
http://www.symantec.com/region/fi/corporate/ids1.html, 17.10.2005

Neohapsis / Archives / IDS List / Message Index / RE: IDS: RE: Info needed to compare Axent ITA and ISS RealSecure. 2000.
http://archives.neohapsis.com/archives/ids/2000-q3/0022.html, 17.10.2005

NFR sentivist version 4. 2003.
http://www.nfr.com/solutions/download/NFR-FS-Data.pdf, 2.3.2006

Oinkmaster features, 2005.
http://oinkmaster.sourceforge.net/features.shtml, 4.11.2005

Panda Software Finland, Rootkit ohjelmat, 2005
http://www.pandasoftware.fi/keskus/artikkeli/rootkit.html, 2005.

Perfmon-graph, 2006. http://people.su.se/~andreaso/perfmon-graph, 17.3.2006

Product reviews – SC magazine US Sourcefire 3D System 2005.
http://www.scmagazine.com/us/products/productdetails/27d31677-e098-4cb8-95eb-099ca79a0f08/sourcefire+3d+system+/, 9.4.2006

Product reviews – SC magazine US Symantec Network Security 2005.
http://www.scmagazine.com/us/products/productdetails/8fc456e3-8cdb-43e3-a633-97d7998b2956/symantec+network+security+7120+/, 9.4.2006

Proventia Intrusion Detection Appliances Datasheet, 2003.

http://documents.iss.net/literature/proventia/Proventia_ASeries_datasheet.pdf, 11.10.2005

Päijät-Hämeen koulutuskonsernin tietoverkko, 2005. http://it.phkk.fi/verkko.html, 19.10.1005

Päijät-Hämeen koulutuskonserni, toimintamalli, 2005. http://www.phkk.fi/esittely, 6.3.2006

Realsecure Network 10/100. 2005. http://documents.iss.net/literature/RealSecure/rsn10-100_datasheet.pdf, 11.10.2005

SANS Institute, The SANS Top 20 Vulnerabilities. 2004. http://www.sans.org/top20, 15.10.2005

Snort Report FAQ, 2005. http://www.symmetrixtech.com/ids/INSTALL, 12.4.2006

Snort Users manual 2.4.0 RC1, 2006. http://www.snort.org/docs/snort_manual/2.4/snort_manual.pdf, 10.11.2005

Sourcefire Network Security – Intrusion Sensor, 2005. http://www.sourcefire.com/products/is.html, 17.10.2005

Symantec Network Security data sheet, 2004. http://enterprisesecurity.symantec.com/content/displaypdf.cfm?pdfid=351&EID=0, 11.10.2005

Symantec Network Security 7100 series, 2005. http://eval.veritas.com/mktginfo/enterprise/fact_sheets/ent-factsheet_network_security_7100_series_01-2005.en-us.pdf, 7.4.2006

The Evolution of Intrusion Detection Systems. 2001.
http://www.securityfocus.org/infocus/1514, 17.10.2005

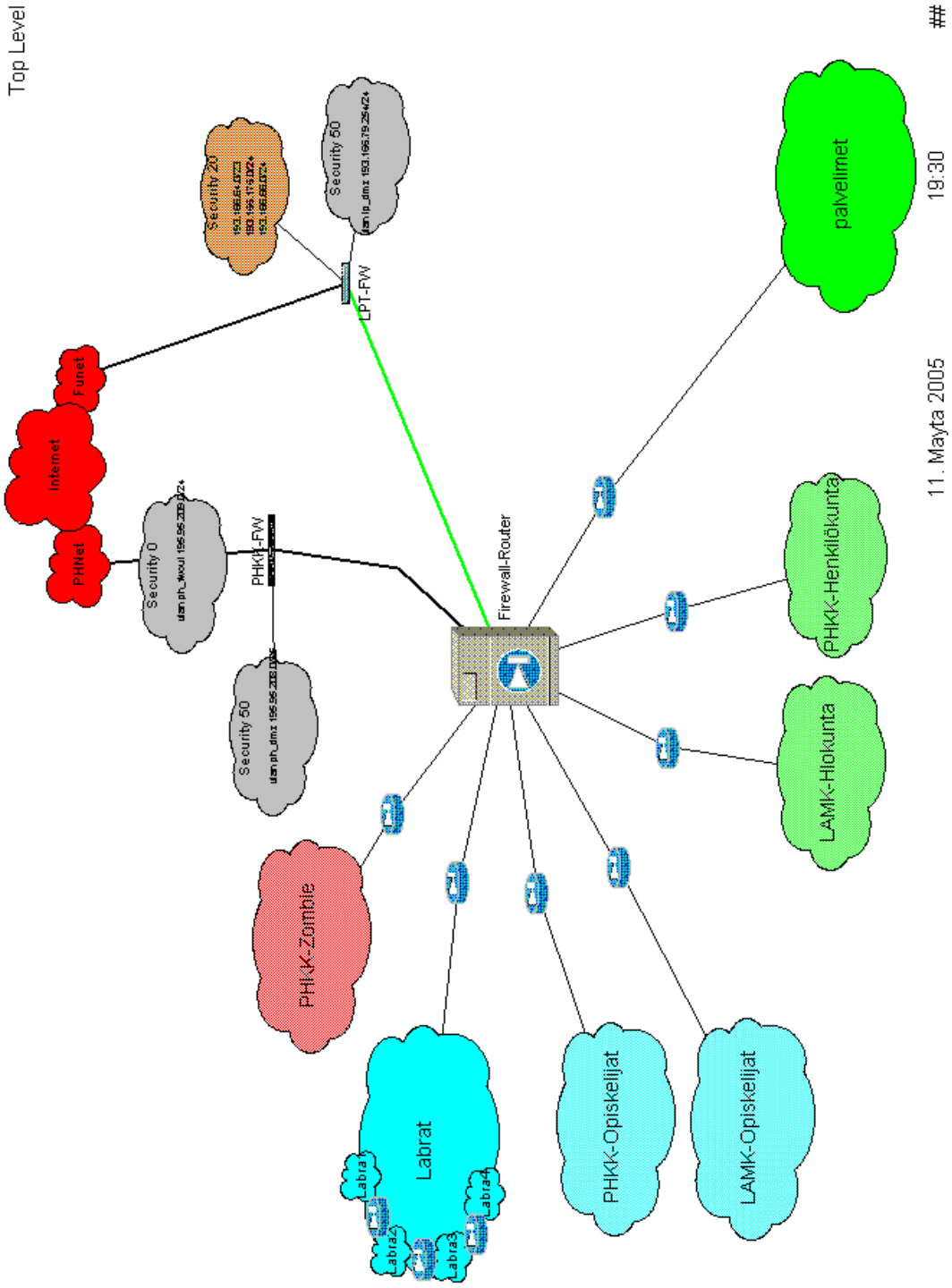
The history of Intrusion Detection at SRI. 2005.
http://www.sdl.sri.com/programs/intrusion/history.html, 17.10.2005

Tunnuslukuja Päijät-Hämeen koulutuskonsernista. 2004.
http://www.phkk.fi/esittely/tunnusluvut/, 6.3.2006

Viestintävirasto 2004a. http://www.ficora.fi/suomi/tietoturva/hyokkays.htm,
2.3.2006

Viestintävirasto 2004b. http://www.ficora.fi/suomi/tietoturva/tekniikat.htm,
2.3.2006

LIITE 1: PHKK:n verkon looginen kuva



LIITE 2: Snort Report:n hälytysraportti

Menu

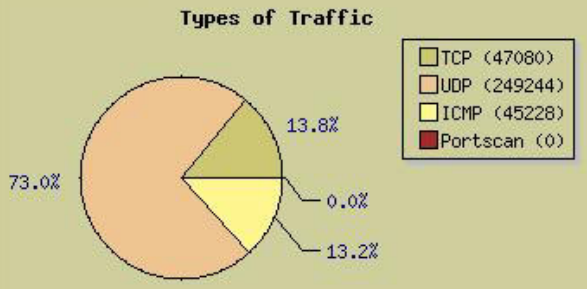
SnortReport

Timeframe: 2005-10-28 01:00:00 **to** 2005-10-29 01:00:00
Current Time: 2005-11-04 09:45:08
Unique Signatures: 83
Number of Alerts: 436455

Earliest Alert: 2005-10-28 01:00:00
Latest Alert: 2005-10-29 00:01:00

Timeframe: GO

Day: GO



Detail by Signatures

Num	Prio	Signature	# Alerts	# Sources	# Dest.	Detail
1	1	BLEEDING-EDGE P2P eDonkey File Status Request [sid 2001297] [url www.edonkey.com]	11511	1	373	Summary
2	1	BLEEDING-EDGE P2P ed2k connection to server [sid 2000330] [url www.giac.org/practical/GCIH/Ian_Gosling_GCIH.pdf]	7426	1	379	Summary
3	1	BLEEDING-EDGE P2P ed2k request part [sid 2000332] [url www.giac.org/practical/GCIH/Ian_Gosling_GCIH.pdf]	2047	2	23	Summary
4	1	BLEEDING-EDGE P2P ed2k file request answer [sid 2000333] [url www.giac.org/practical/GCIH/Ian_Gosling_GCIH.pdf]	1370	2	226	Summary
5	1	NETBIOS SMB-DS Session Setup AndX request unicode username overflow attempt [sid 2404] [url www.eeye.com/html/Research/Advisories/AD20040226.html] [bugtraq 9752]	198	18	55	Summary
6	1	BLEEDING-EDGE Malware JoltID Agent Keep-Alive [sid 2001015] [url securityresponse.symantec.com/avcenter/venc/data/adware.p2pnetworking.html] [url forum.treweeke.com/lofiversion/index.php/t597.html] [url www.joltid.com]	133	1	4	Summary
7	1	BLEEDING-EDGE P2P Gnutella Connect [sid 2001664] [url www.gnutella.com]	75	1	59	Summary
8	1	BLEEDING-EDGE Potential MySQL bot scanning for SQL server [sid 2001689] [url isc.sans.org/diary.php?date=2005-01-27]	70	1	2	Summary
9	1	BLEEDING-EDGE POLICY MSN status change [sid 2002192]	66	6	10	Summary
10	1	BLEEDING-EDGE Malware JoltID Agent Probing or Announcing UDP [sid 2000900] [url securityresponse.symantec.com/avcenter/venc/data/adware.p2pnetworking.html] [url forum.treweeke.com/lofiversion/index.php/t597.html] [url www.joltid.com]	29	1	8	Summary
11	1	BLEEDING-EDGE P2P eDonkey File Status [sid 2001296] [url www.edonkey.com]	22	1	4	Summary
12	1	NETBIOS SMB Session Setup AndX request unicode username overflow attempt [sid 2403] [url	19	5	8	Summary

LIITE 3: Snortin asennusohje

Snort_Enterprise_Install

Snort, Apache, SSL, PHP, MySQL, and BASE Install on CentOS 4, RHEL 4 or Fedora Core

By Patrick Harper | CISSP RHCT MCSE

with contributions and editing by Nick Oliver | CNE

http://www.InternetSecurityGuru.com

BASE – Basic Analysis and Security Engine

Introduction:

This is really a deviation from what I have done before. It will start from a minimal install of CentOS 4 or RHEL 4 and will build a Snort sensor/manager. This system will start at the command line and not have X window installed unless you add it during the install. Also you can use Fedora with very little change to this doc.

Acknowledgments:

I would like to thank all my friends and the people on the Ntsug-Users list that proofed this for me. My wife Kris, Nick Oliver (He downloaded and used the first document I wrote and volunteered to do test installs and proof the spelling and punctuation for the following documents. He has become quite proficient with Linux and Snort and is a valued member of the ISG team and contributor to this and other documentation. I would also like to thank the people from the snort-users list and ntsug-users list that helped.

Also I would like to thank Marty and the Snort team for their great work. Thanks for staying true to open source.

Comments or Corrections:

Please e-mail any comments or corrections to
mailto:Patrick@internetsecurityguru.com
Nick Oliver has also made himself available for contact if for any reason I may be unavailable or running behind on my large and ever growing inbox.
mailto:nwoliver@internetsecurityguru.com

The latest version of this document is located at http://www.internetsecurityguru.com/documents/.

LIITE 3 JATKUU

Please use the most up to date version I will do my best to keep it updated.

Info for the install:

IP Address
Subnet Mask
Gateway
DNS Servers
Hostname

Other important reading:

Snort users manual http://www.Snort.org/docs/writing_rules/
Snort FAQ http://www.Snort.org/docs/faq.html
The Snort user's mailing list http://lists.sourceforge.net/lists/listinfo/snort-users
This is the place to get help AFTER you read the FAQ,, ALL the documentation on the
Snort website, AND have searched Google).
Also make sure to read the link below before sending questions. It helps to know the
rules. ☺
The Snort drinking game
http://www.theadamsfamily.net/~erek/snort/drinking_game.txt (Thanks Erek)
Websites to visit:
http://www.snort.org
http://secureideas.sourceforge.net/
http://www.mysql.com
http://www.php.net
http://www.centos.org
http://www.chiark.greenend.org.uk/~sgtatham/putty/ (the putty SSH client)
http://www.bastille-linux.org (Hardening scripts for UNIX and Linux)
http://www.internetsecurityguru.com (**my website**)
If you follow this doc line by line, it will work for you. Over 90% of the e-mails I get are from people who miss a step. However, I always welcome comments and questions and will do my best to help whenever I can.

Installing CentOS 4:

We will install a minimal number of packages, sufficient for a usable system. After the install we'll turn off anything that is not needed. By hardening the OS and further securing the system, it will be ideal as a dedicated IDS. It is, however, also a system that can easily be added to for other uses. There are lots of good articles on how to secure a Redhat/Fedora box on the web. Just go to http://www.google.com and search for "securing redhat" or visit http://www.bastille-linux.org/ .
You will start at a grub screen that has boot:, hit enter. Then you can either choose to check your cd's or skip. If you know they are good then skip it otherwise you might want to check them out.

Welcome:
Click next

LIITE 3 JATKUU

Language:
English

Keyboard:
U.S. English

Install Type:
Choose custom

Disk Partitioning:
Choose to automatically partition the hard drive.
Choose to remove all partitions from this hard drive (I am assuming that this not a dual boot box)
Make sure the review button is checked
When the warning dialog comes up, choose Yes.
Accept the default layout. Most of the disk will be /

Boot Loader:
Go with the default (if this is a dual boot system then go to google and search for info on how to install grub for dual booting)

Network Configuration:
Hit edit, Uncheck "Configure with DHCP", Leave "Activate on boot"
Set a static IP and subnet mask for your network
Manually set the hostname
Set a gateway and the DNS address(s)

Always try to assign a static IP address here. I think it is best not to run Snort off of a Dynamic IP, however, if you need to, go ahead and do it, just make sure to point your $HOME_NET variable in your Snort.conf to the interface name. You can get more info on that in the Snort FAQ. If this is a dedicated IDS then you do not need to have an IP on the interface that Snort is monitoring (for tips on setting up snort with two NIC's see the bottom of this doc).

Firewall:
Choose "enable firewall"
Select remote login (SSH) and Web Server (HHTP, HTTPS)
For the SELinux option, move to warn.

Additional Language:
Choose only US English

Time Setup:
Choose the closest city within your time zone (for central choose Chicago)

Root Password:
Set a strong root password here (a strong password has at least 8 characters with a

combination of upper case, lower case, numbers and symbols. It should also not be, or resemble, anything that might be found in a dictionary of any language)

Suggested Packages:
Take the defaults with the following exceptions. (Default is what ever it has when you choose custom; for example, gnome is checked by default and KDE is not)

Desktops:
X Window System – unchecked
Gnome Desktop Environment – unchecked
KDE Desktop Environment - unchecked
XFCE - Accept the default unchecked

Applications:
Editors – choose VIM (or anything else you want to use under this tab)
Engineering and Scientific – Accept the default (unchecked)
Graphical Internet – unchecked
Text based internet – checked by default, leave it this way
Office/Productivity – unchecked.
Sound and Video – unchecked
Authoring and Publishing – unchecked
Graphics – make sure it is unchecked
Games and Entertainment – unchecked

Server Section:
Server configuration tools
• Check and leave at the default
Web Server – ONLY the following should be checked
• Crypto-Utils
• Mod_auth_mysql
• Mod_perl
• Mod_ssl
• Php
• Php_mysql
• Webalizer (if you want to be able to view your web logs graphically)
Mail Server – none
Windows File Server – None
DNS server – None
FTP server – None
Postgresql Database - None
MySQL Database– Check only the following
• MyODBC
• Mod_auth_mysql
• Mysql-devel
• Mysql-server
• Mysqlclient10
• Perl-DBD-MySQL

LIITE 3 JATKUU

• Php-mysql
News server – none
Network Servers – None
Legacy network servers – None

Development:
Development tools – check this one and click "details" and check the following in addition to what is checked by default
• Expect
• Gcc-objc

X Software Development – leave this unchecked
Gnome Software Development – Leave this unchecked
KDE Software Development – Leave this unchecked
XFCE Software Development – Leave unchecked
Legacy Development – Leave unchecked

System:
Administration – check and accept default
System Tools – unchecked:
Printing support – unchecked

Miscellaneous:
Choose nothing from this entire section
Hit next, then next again. It will tell you that you will need 3 CD's. Hit continue and the install will start. First it will format the drive(s) and then it will install the packages. This will take a little while, depending on the speed of the system you're on, so putting on a pot of coffee is good right about here.

Installing extra software:
You can install almost anything, but remember, if this system is located outside your firewall, is your production IDS, or if you want it really secure, you will want to install the least amount of software possible.

Each piece of software you install and forget to update and maintain is a vulnerability waiting to happen, and that goes for all systems. To me this is one of the most fundamental rules of systems administration. Make sure you know what you have, and make sure you keep it patched and secured so you do not contribute to the next worm, virus, or hacking spree that threatens to shut down major portions of the internet.
If this is a production system, please make sure you learn how to secure it. Otherwise it will not be your system for long

After the packages install:
Reboot – hit the reboot button
After the reboot:

LIITE 3 JATKUU

You are now in runlevel 3 – command line only

Login as root and setup a user account for yourself

User Account:
Add a user account for yourself here; make sure to give it a strong password
The root account should not be used for everyday use, if you need access to root functions then you can "su -" or "sudo" for root access. (For help with sudo visit google.com)

groupadd <groupname>
useradd –g <username> <groupname>

Associate a password with this new username

passwd <username>

You will then be asked to enter and then confirm a password. You can now login as a normal user and, if necessary, if you want root privileges, use su – .

Disable unneeded services:

Disable apmd, cups, isdn, netfs, nfslock, pcmcia (unless you are using a laptop), portmap by typing (as root):
Chkconfig <service> off
You will do this for each service to be terminated.

Update your system

We will be using Yum to keep the system up to date. First we will have to import the GPG key. At the command line type:

rpm --import http://mirror.centos.org/centos/RPM-GPG-KEY-CentOS-4

Then type "yum -y update" and it will check what you need and install it.
(Type "chkconfig yum on" and "service yum start" to turn on nightly updates, this is a suggested step)

You will need to reboot after this because a new kernel will have been installed during the yum update.

You are now ready to start installing Snort and all of the software it needs. You can either do this from the command line, or SSH into the server from another box. Either will work fine. For the novice it might be easier to do this from SSH so they can cut and paste the commands from this document into the session, instead of typing some of the long strings.

LIITE 3 JATKUU

Preparing for the install:

Again, if you are not logged in as root, then you will need to su to root ("su -" will load the environmental variables of root. Use that when you su.). Ensure that you have downloaded all of the installation files before you start the install, it will go smoother, trust me. Go to your download directory and start with the following procedures.

Securing SSH

In the /etc/ssh/sshd_config file change the following lines (if it is commented out remove the #):

Protocol 2
PermitRootLogin no
PermitEmptyPasswords no

Save the file and type "service sshd restart". SSH will restart, enacting these changes. (You will need to SSH into the box with the user account you created after this, as root will no longer be accepted. Just "su –" to the root account)

Turn on and set to start the services you will need

chkconfig httpd on
chkconfig mysqld on
service httpd start
service mysqld start

Testing Apache

Install the Network Query Tool, using http://shat.net/php/nqt/nqt.php.txt. Copy the text into a file called query.php and place it in the /var/www/html directory.

Download all the needed files:

Place all the downloaded files into a single directory for easy access and consolidation. This directory will not be needed when you are finished with the installation and may be deleted at that time. I create a directory under /root called snortinstall. From the command line type:

cd /root
mkdir snortinstall

Remember, you can always check where you are currently by typing "pwd" at the command line. Note: If you are not logged in as root, then you will need to execute "su –" ("su" gives you the super user or root account rights, the "–" loads the environmental variables of the root account for you) and then enter the root password.

!!!DO THE FOLLOWING AS ROOT!!!

LIITE 3 JATKUU

Use wget (wget will place the file you're downloading into the directory where you're currently located) to download these files. To use wget, type "wget <URL_to_file>", and it will begin the download to the directory that you are currently in. If you want to use a Windows box and need an SSH client, then you can go to the PuTTY http://www.chiark.greenend.org.uk/~sgtatham/putty/ home page and download a free one. This is for windows machines to SSH to Linux/UNIX box's
OR:
http://ftp.ssh.com/pub/ssh/SSHSecureShellClient-3.2.9.exe for a client that can both SSH and start an SCP connection to the box you have SSH'd to from within the session. This is free for non-commercial use and pretty nice.

Download Snort and PCRE
Use wget from the command line or an SSH terminal window. From inside of the /root/snortinstall directory, type:

wget http://www.snort.org/dl/current/snort-2.4.3.tar.gz

When that is downloaded, type:

wget http://easynews.dl.sourceforge.net/sourceforge/pcre/pcre-5.0.tar.gz

Install PCRE from source
tar –xvzf pcre-5.0.tar.gz
cd pcre-5.0
./configure
make
make install

Installing and setting up Snort and the Snort rules:

cd back to your snortinstall dir (cd ~/snortinstall)
tar -xvzf snort-2.4.3.tar.gz
cd snort-2.4.3
./configure --with-mysql
make
make install

groupadd snort
useradd -g snort snort –s /sbin/nologin

Then:

mkdir /etc/snort
mkdir /etc/snort/rules
mkdir /var/log/snort
cd etc/
cp * /etc/snort

LIITE 3 JATKUU

From your snortinstall dir (cd /root/snortinstall) :
wget http://www.snort.org/pub-bin/downloads.cgi/Download/vrt_pr/snortrules-pr-2.4.tar.gz

Then tar –xvzf snortrules-pr-2.4.tar.gz
cd to rules and do the following command
cp –R * /etc/snort/rules

Modify your snort.conf file

The snort.conf file is located in /etc/snort, make the following changes.

var HOME_NET 10.2.2.0/24 (make this what ever your internal network is, use CIDR. If you do not know CIDR then go to http://www.oav.net/mirrors/cidr.html)

var EXTERNAL_NET !$HOME_NET (this means everything that is not your home net is external to your network)

change "var RULE_PATH ../rules" to "var RULE_PATH /etc/snort/rules"

After the line that says "preprocessor stream4_reassemble" add a line that looks like

"preprocessor stream4_reassemble: both,ports 21 23 25 53 80 110 111 139 143 445 513 1433" (without the quotes)

Now tell snort to log to MySQL
Go down to the output section and uncomment the following line. Change it to be like the following except the password. Remember what you make it because you will need it later when you set up the snort user in mysql.

output database: log, mysql, user=snort password=<the password you gave it> dbname=snort host=localhost

Get snort start with the system

Change directory to /etc/init.d and type:
wget http://internetsecurityguru.com/snortinit/snort
chmod 755 snort
chkconfig snort on.

Setting up the database in MySQL:

I will put a line with a > in front of it so you will see what the output should be. (Note: In MySQL, a semi-colon " ; " character is mandatory at the end of each input line)
('password' is whatever password you want to give it, just remember what you assign.

LIITE 3 JATKUU

For the snort user use what you put in the output section of the snort.conf in the section
above)

```
mysql
mysql> SET PASSWORD FOR root@localhost=PASSWORD('password');
>Query OK, 0 rows affected (0.25 sec)
mysql> create database snort;
>Query OK, 1 row affected (0.01 sec)
mysql> grant INSERT,SELECT on root.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql> SET PASSWORD FOR snort@localhost=PASSWORD('password_from_snort.conf');
>Query OK, 0 rows affected (0.25 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort;
>Query OK, 0 rows affected (0.02 sec)
mysql> exit
>Bye
```

Execute the following commands to create the tables

mysql -u root -p < ~/snortinstall/snort-2.4.3/schemas/create_mysql snort
Enter password: the mysql root password

Now you need to check and make sure that the Snort DB was created correctly

```
mysql -p
>Enter password:
mysql> SHOW DATABASES;
(You should see the following)
+------------+
| Database
+------------+
| mysql
| Snort
| test
+------------+
3 rows in set (0.00 sec)

mysql> use snort
>Database changed
mysql> SHOW TABLES;
+------------------+
| Tables_in_snort
+------------------+
| data
| detail
| encoding
| event
| icmphdr
```

| iphdr
| opt
| reference
| reference_system
| schema
| sensor
| sig_class
| sig_reference
| signature
| tcphdr
| udphdr
+------------------+
16 rows in set (0.00 sec)
exit;

BASE Install

Go to your snort download directory (cd /root/snortinstall)

Type “yum install php-gd” this will install gd for proper graphing in BASE

It will ask you the following, choose Y

Transaction Listing:
Install: php-gd.i386 0:4.3.10-3.2
Is this ok [y/N]: y

Download ADODB
wget http://easynews.dl.sourceforge.net/sourceforge/adodb/adodb462.tgz

Download BASE
wget http://easynews.dl.sourceforge.net/sourceforge/secureideas/base-1.2.tar.gz

Hand configure your firewall:
cd /etc/sysconfig/
edit the iptables file
add the line “-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j
ACCEPT
And delete the lines:
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
Then change the line :
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT

LIITE 3 JATKUU

To :
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j REJECT

Then you will only be able to get to the site with HTTPS:// the reason you want to do this is so you do not trigger more alerts from you reading alerts, and if something is able to be encrypted then I usually do.

Then execute the command "service iptables restart" and you will see something like tee following:

[root@snort conf]# service iptables restart
Flushing firewall rules: [OK]
Setting chains to policy ACCEPT: filter [OK]
Unloading iptables modules: [OK]
Applying iptables firewall rules: [OK]

Then it will look like this when you do an "iptables –L"

[root@snort ~]# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
RH-Firewall-1-INPUT all -- anywhere anywhere
Chain FORWARD (policy ACCEPT)
target prot opt source destination
RH-Firewall-1-INPUT all -- anywhere anywhere
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Chain RH-Firewall-1-INPUT (2 references)
target prot opt source destination
ACCEPT all -- anywhere anywhere
REJECT icmp -- anywhere anywhere icmp any reject-with icmp-port-unreachable
ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED
ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ssh
ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:https
REJECT all -- anywhere anywhere reject-with icmp-host-prohibited

Installing ADODB:

Go back to your download directory (~/snortinstall)
cp adodb462.tgz /var/www/
cd /var/www/
tar -xvzf adodb462.tgz
rm –rf adodb462.tgz

Installing and configuring BASE:

Go back to your download directory (~/snortinstall)
cp base-1.2.tar.gz /var/www/html
cd /var/www/html
tar –xvzf base-1.2.tar.gz
rm –f base-1.2.tar.gz
mv base-1.2 base (this renames the base-1.2 directory to just "base")

```
cd /var/www/html/base
```

LIITE 3 JATKUU

cp base_conf.php.dist base_conf.php

edit the “base_conf.php” file and insert the following perimeters

$BASE_urlpath = "/base";

$DBlib_path = "/var/www/adodb/ ";
$DBtype = "mysql";

$alert_dbname = "snort";
$alert_host = "localhost";
$alert_port = "";
$alert_user = "snort";
$alert_password = "password_from_snort_conf";

/* Archive DB connection parameters */
$archive_exists = 0; # Set this to 1 if you have an archive DB

Now, go to a browser and access your sensor.

NOW: “chkconfig snort on” to make snort starts with the system
then type service snort start. It should give you an OK

https://<ip.address>/base

This will bring up the initial BASE startup banner.

Click the “setup page” link, then on the resulting page, click on the setup AG button.

Click the main page on the bottom and you should see the BASE page

Securing APACHE and the BASE directory:

mkdir /var/www/passwords

/usr/bin/htpasswd -c /var/www/passwords/passwords base

(base will be the username you will use to get into this directory, along with the password you choose)
It will ask you to enter the password you want for this user, this is what you will have to type when you want to view your BASE page

Edit the httpd.conf (/etc/httpd/conf). I put it under the section that has:

<Directory />
Options FollowSymLinks

LIITE 3 JATKUU

AllowOverride None
</Directory>

These are the lines you must add to password protect the BASE console, add it to the httpd.conf file in /etc/httpd/conf/:

<Directory "/var/www/html/base">
AuthType Basic
AuthName "SnortIDS"
AuthUserFile /var/www/passwords/passwords
Require user base
</Directory>

Since you have removed the port 80 entry in the iptables script you will have to go to the console on port 443, using HTTPS:/<ip_address>/base

Save the file and restart Apache by typing "service httpd restart" to make the password changes effective.

After you're done

Login as root and check everything important to see if it is running.

To check you can execute "ps –ef |grep <SERVICE>" where service is snort. httpd, or mysql.

Or use "ps –ef |grep httpd && ps –ef |grep mysql && ps –ef |grep Snort"

Now it's time to test Snort. I suggest using something free like GFI Languard – a real good program that is cheap (http://www.gfi.com/languard/) or Nessus – a real good program that is free (http://www.nessus.org) if you have it, and running it against your Snort box. Check BASE when you're done and it should have a bunch or alerts. If you are on DSL or cable then you could already have a bunch in there right after you start it up. When you go to the BASE screen in your browser now you should see alerts (And this is without running any programs against it) Now you need to tune your IDS for your environment. This is an important step. Look at the Snort list archives and the other links listed above and you will find good tips on how to do that.

There is also a very good book out on Snort for those that want to learn more about it.
http://www.amazon.com/exec/obidos/tg/stores/detail/-/books/1931836744/
And a few others listed at http://www.Snort.org/docs/#Snort_books

Troubleshooting (the Snort install)

If you are having trouble type the following

LIITE 3 JATKUU

snort –c /etc/snort/snort.conf

It will give you output that will be helpful. It will tell you if you are having problems with rules or if you have a bad line in your conf file. If you do this and read the output you will be able to fix most of the problems I get e-mailed with.
Next, this is an end-to-end guide. I designed it to take a system from bare metal to functional IDS. If you follow it step by step you will get an IDS working, then you customize it more. I have the Fedora install listed the way I do because there are some parts that are needed.
If you do not have a sensor number, it means that you have not received an alert on that sensor yet. Make sure everything is running without error and check BASE again
If you are getting nothing in BASE you could have a number of problems. Check your /var/log/snort directory and see if you have an alert file. If it has alerts, then Snort is working and you most likely do not have your Snort.conf output lines correct. Check where you setup your database in it first. If you do not have an alert file then make sure Snort is running. If it is, make sure that if you are on a switch, you are on a span (or mirrored) port, or you will not see anything but what is destined for that port. Scan you box with Nessus or CIS before you start getting worried.

The best place to look for other answers is the Snort-users archive, which is indexed by Google. If you are not proficient at searching, I would suggest reading http://www.google.com/help/basics.html . It is a good primer, as is http://www.googleguide.com/

Read what is out there for you. Go to http://www.snort.org and look around. http://www.snort.org/docs/snort_manual/ is also something you should read all the way through, as well as http://www.snort.org/docs/FAQ.txt between them and Google almost all your questions will be answered.

Most of the problems people have had stem from them missing a step, frequently only one step, somewhere. There are a lot of them and it is easy to do.

If you do have problems feel free to e-mail me, Nick, or the Snort-users list.

There is a huge community of people out there using this product that will help you if you are in trouble. Remember, however, that this support is free and done out of love of this product. You certainly should not expect the same response from the Snort community as you would from an IDS vendor (though I have gotten better response time from the Snort-users list than I have from some vendors in the past)

Hope this gets you going. If not, then feel free to e-mail either myself, Nick Oliver, or the Snort-users list. They are a great bunch of people and will do all

they can for you (if you have manners). Just remember, however, that it is a volunteer thing, so you will probably not get answers in 10 minutes. DO NOT repost your question merely because you have not yet seen an answer, this is free support from the goodness of peoples hearts. They help you out as fast as they can.

Good luck and happy Snorting.

Reboot your system; watch to make sure everything starts. You can check by doing a "ps –ef |grep <service>" the service can be any running process. i.e. mysql, httpd, Snort, etc.

Two NIC's in the Pig

You may want to have one interface for management and one for sniffing, this is a good thing to do. Here is an example config

cd /etc/sysconfig/network-scripts/

Here you have a file for each of your interfaces (ifcfg-ethX)

For your sniffing interface make the file say the following:
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet

For your management make it say this: (with your info of course)
DEVICE=ethX
BOOTPROTO=none
HWADDR=00:08:C7:56:E8:87
ONBOOT=yes
TYPE=Ethernet
HOSTNAME=snort.whatever.com
IPADDR=10.10.10.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
GATEWAY=10.10.10.1
IPV6INIT=no

OinkMaster

Please see the OinkMaster install doc on my website

Coming soon is a barnyard doc and a doc on how to deploy multiple sensors with one base station and have them all communicate securely.

LIITE 4: Bro:n hälytysraportti

```
Site Report for bro-kone, from 2005/10/28 00:00:30 to 2005/10/29
00:00:30
generated on Sat Oct 29 00:12:01 2005
================================================================
======
Summary
================================================================
======
  Incidents
    Likely Successful     101
    Unknown               0
    Likely Unsuccessful   46

  Scanning Hosts
    Successful            11
    Unsuccessful          0

  Signature Summary
    Total signatures          9723
    Unique signatures         9
    Unique sources            27
    Unique destinations       126
    Unique source/dest pairs  147

================================================================
======
Signature Distributions
================================================================
======
                                        Unique      Unique
Unique
  Signature ID                Count     Sources     Dests
Pairs
  ------------------------  ---------  ---------  ---------  -----
------
  s2b-279-3                 8839       15         51         65
  s2b-1413-10               859        1          68         68
  s2b-1980-1                7          2          2          2
  s2b-1365-5                6          3          4          4
  s2b-518-6                 4          4          1          4
  s2b-1983-1                3          3          2          3
  s2b-1213-5                2          1          1          1
  s2b-1087-8                2          1          1          1
  s2b-1981-1                1          1          1          1

================================================================
======
Incident Details
================================================================
======
                  # legend for connection type #
                  ------------------------------
         C Connection Status
           # number corresponds to alarm triggered by the connec-
tion
           * successful connection, otherwise unsuccessful.
         I Initiatator of Connection
           > connection initiated by remote host
           < connection initiated by local host
```

LIITE 4 JATKUU

```
------------------------------------------------------------------
------
Incident      prvphkk-000041                              LIKELY
SUCCESSFUL
------------------------
Remote Host:  192.168.xxx.xxx
 Local Host:  193.166.xxx.xxx

Alarm: SensitiveSignature
  1   s2b-279-3: 192.168.xxx.xxx: DOS Bay/Nortel Nautica Marlin
      Duplicates suppressed: 159
      10/28 00:05:17               192.168.xxx.xxx ->
193.166.xxx.xxx
                                          4790/udp -> 161/udp
      signature code:
        signature s2b-279-3 {
          ip-proto == udp
          dst-port == 161
          payload-size == 0
          event "DOS Bay/Nortel Nautica Marlin"
        }

Connections (only first 25 after alarm are listed)
-----------
                 time     byte   remote        local   byte
 date   time   duration transfer  port  C   I   port transfer
protocol
----- -------- -------- -------- ------ ------ ----- -------- ----
------
10/28 00:04:15 0.003185      110   4790 1    >   161      110
other
10/28 00:14:19 0.000916       42   1152 *    >   161       46
other
10/28 00:14:19 0.001978      110   1154 *    >   161      110
other
10/28 00:24:23 0.000876       42   1483 *    >   161       46
other
10/28 00:24:23 0.001943      110   1485 *    >   161      110
other
10/28 00:34:13 0.000910       42   1815 *    >   161       46
other
10/28 00:34:13 0.002082      110   1818 *    >   161      110
other
10/28 00:44:17 0.000932       42   2157 *    >   161       46
other
10/28 00:44:17 0.003239      110   2159 *    >   161      110
other
10/28 00:54:21 0.000885       42   2488 *    >   161       46
other
10/28 00:54:21 0.002298      110   2489 *    >   161      110
other
10/28 01:04:10 0.000932       42   2823 *    >   161       46
other
10/28 01:04:10 0.002164      110   2826 *    >   161      110
other
10/28 01:14:14 0.000895       42   3159 *    >   161       46
other
10/28 01:14:14 0.002034      110   3161 *    >   161      110
other
```

LIITE 4 JATKUU

```
10/28 01:24:19 0.000881       42   3484 *    >   161       46
other
10/28 01:24:19 0.004498      110   3490 *    >   161      110
other
10/28 01:34:23 0.000888       42   3832 *    >   161       46
other
10/28 01:34:23 0.002096      110   3833 *    >   161      110
other
10/28 01:43:30 0.072767        ?      8      >     0        ?
other
10/28 01:43:30 0.072651        ?      0     <      0        ?
other
10/28 01:43:30 19.99897      273   1840      >   161        ?
other
10/28 01:44:00 19.99920      192   2062      >   161        ?
other
10/28 01:44:13 0.000820       42   2162 *    >   161       46
other
10/28 01:44:13 0.002006      110   2163 *    >   161      110
other
------------------------------
```

LIITE 5: BASE:n yksittäinen hälytys

Meta

ID #	Time	Triggered Signature
6 - 809301	2006-03-28 04:00:27	[url] [local] [snort] BLEEDING-EDGE Potential SSH Scan

Sensor	Name	Interface	Filter
	nids.prv.phkk.fi		*none*

Alert Group: *none*

IP

Source Address	Dest. Address	Ver	Hdr Len	TOS	length	ID	flags	offset	TTL	chksum
59.106.12.187	193.166.[redacted]	4	20	0	60	56739	2	0	47	5435

Options: *none*

TCP

Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	seq #	ack	offset	res	window	urp	chksum
35654 [sans] [portsdb] [tantalo] [sstats]	22 [sans] [portsdb] [tantalo] [sstats]							X		2246075015	4188364158	10	0	5840	0	14631

Options: *none*

Payload

Plain Display

Download of Payload

none